Lower Bounds for Unitary Property Testing with Proofs and Advice

Jordi Weggemans

QuSoft & CWI, Amsterdam, the Netherlands

In unitary property testing a quantum algorithm, also known as a *tester*, is given query access to a black-box unitary and has to decide whether it satisfies some property. We propose a new technique for proving lower bounds on the quantum query complexity of unitary property testing and related problems, which utilises its connection to unitary channel discrimination. The main advantage of this technique is that all obtained lower bounds hold for any C-tester with $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$, showing that even having access to *both* (unentangled) quantum proofs and quantum advice does not help for many unitary property testing problems.

We apply our technique to prove lower bounds for problems like quantum phase estimation, the entanglement entropy problem, quantum Gibbs sampling and more, removing all logarithmic factors in the lower bounds obtained by the sample-to-query lifting theorem of Wang and Zhang (2023). As a direct corollary, we show that there exist quantum oracles relative to which $\mathsf{QMA}(2) \not\supset \mathsf{SBQP}$ and $\mathsf{QMA}/\mathsf{qpoly} \not\supset \mathsf{SBQP}$. The former shows that, at least in a black-box way, having unentangled quantum proofs does not help in solving problems that require high precision.

1 Introduction

Quantum query complexity is the study of how many queries a quantum algorithm has to make to some black-box input X to decide whether X satisfies some property $\mathcal{P}$. Whilst quantum query complexity conventionally focuses on X being inherently classical (i.e., a classical bit string), it is also possible to consider the setting where X is some black-box unitary. Whilst the former (which we call classical property testing) is very useful in obtaining insights into the differences in computational power between different classes of computation, classical or quantum, the latter (called unitary property testing) gives another way to compare inherently quantum classes. These problems, first studied by Wang [1], got considerably more attention recently [2, 3, 4].

Query complexities can vastly differ among different classes of computational models. For example, the search problem, which is to decide whether a string of length N is either the all-zeros string or has at least one entry with a '1', is known to have classical query complexity of $\Theta(N)$ and quantum query complexity of $\Theta(\sqrt{N})$ [5, 6]. However, given a string by an untrusted prover, the query complexity of the search problem is just 1 in both cases. A similar result holds for a unitary property testing analogue of search as introduced by Aaronson and Kuperberg [7], where one has to decide whether a given black-box unitary

Jordi Weggemans: jrw@cwi.nl, https://jordiweggemans.github.io

U applies either the identity operation $\mathbb{I}$ or the reflection $\mathbb{I} - 2|\psi\rangle\langle\psi|$ for some unknown N-dimensional quantum state $|\psi\rangle$. This problem has in general a quantum query complexity of $\Theta(\sqrt{N})$, but can again be solved by just a single query if a *quantum state* is provided by an untrusted prover as an extra input. For many other unitary property testing problems, it is unclear whether quantum proofs and/or trusted advice states might help in solving these tasks.

Our main contribution is a new lower bound technique for query complexity of unitary property testing in the presence of *both* (quantum) proofs and advice, based on the connection between unitary property testing and the discrimination of unitary quantum channels, a topic widely studied in quantum information theory [8, 9, 10, 11].

1.1 Unitary property testing lower bounds by unitary channel discrimination

Following the definition of She and Yuen [2], a unitary *property testing* problem $\mathcal{P}$ consists of two disjoint sets of d-dimensional unitaries $\mathcal{P}_{\text{yes}}$ and $\mathcal{P}_{\text{no}}$ for a fixed dimension d. For some unknown input unitary U, given the promise that either (i) $U \in \mathcal{P}_{\text{yes}}$ or (ii) $U \in \mathcal{P}_{\text{no}}$, the task is to decide whether (i) or (ii) holds by making (controlled) queries to U or its inverse. Similarly, in unitary channel *discrimination* one is also given black-box access to an unknown unitary U promised to be from a known set of candidate unitaries, also known as hypotheses, from which one has to decide which one corresponds to U. When the hypothesis set consists of two families of unitaries $\{U_1 : U_1 \in \mathcal{P}_{\text{yes}}\}$ and $\{U_2 : U_2 \in \mathcal{P}_{\text{no}}\}$ for some property $\mathcal{P}$, discriminating between any $U_1 \in \mathcal{P}_{\text{yes}}$ and $U_2 \in \mathcal{P}_{\text{no}}$ allows one to solve the property testing problem.

We consider quantum query algorithms for property testing (also known as C-*testers*, where C refers to a complexity class) according to the following model: starting with an initial state $|\psi_{\text{init}}\rangle$, the tester is allowed to make queries to U interleaved with applications of unitaries V_t that do not depend on the input, and finally makes a two-outcome measurement to decide with high probability whether $U = U_1$ or $U = U_2$. Again, the queries to U can be controlled, applications of the inverse, or a combination of both. The types of initial states we consider are of the form $|\psi_{\text{init}}\rangle = |0\rangle^{\otimes \mathsf{poly}(n)} |\psi_{\text{input}}\rangle$, where $|\psi_{\text{input}}\rangle$ depends on the class of property testers considered. For example, a BQP-tester has no input state, a $\mathsf{BQP/qpoly}$-tester has $|\psi_{\text{input}}\rangle = |\psi_n\rangle$, where $|\psi_n\rangle$ is some trusted quantum state which only depends on the input length (defined below), and a QMA-tester has $|\psi_{\text{input}}\rangle = |\xi\rangle$ for some untrusted quantum proof $|\xi\rangle$. The strongest advice/proof model we consider is then a $\mathsf{QMA}(2)/\mathsf{qpoly}$-tester, which uses both a polynomial number of unentangled quantum proofs and a quantum advice state as extra input to the computation.

It is well-known that the one-shot distinguishability (i.e. when one can only apply the quantum channel once) is characterised by the so-called diamond distance between U_1 and U_2, denoted as $\frac{1}{2}\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\|_\diamond$.[1] The diamond norm can be computed via a semidefinite program [12], and allows for simplified expressions when the channels are unitaries [11]. Having controlled access to a unitary can make two indistinguishable channels perfectly distinguishable. Take for example $U_1 = \mathbb{I}$ and $U_2 = -\mathbb{I}$: we have that $\frac{1}{2}\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\|_\diamond = 0$, but $\frac{1}{2}\|\mathcal{U}(cU_1) - \mathcal{U}(cU_2)\|_\diamond = 1$, where $cU_i = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_i$ for $i \in \{1, 2\}$. A circuit which achieves perfect discrimination is one which applies cU_i to the Bell state $|\Phi^+\rangle$ and performs a measurement in the Bell basis. However, in this simple example, the power of the controlled application of U can easily be removed by applying a global phase to one of the unitaries, such that now $U_1 = U_2 = \mathbb{I}$, making them indistinguishable even in the

[1] This notation is used to make a distinction between the unitary U and its corresponding channel $\mathcal{U}(U) : \rho \to U^\dagger \rho U$, where ρ is a density matrix.

controlled setting. As it turns out, adding this variable global phase to one of the unitaries (which is fine in our lower bound method, since we have the freedom to choose our U_1 and U_2) allows one to show that access to the inverse, controlled access, or a combination of both, does not increase the ability to discriminate both unitaries.

Using the above ideas, our main theorem is a lower bound on the query complexity of any quantum algorithm, given access to multiple unentangled quantum proofs and quantum advice, that discriminates between the unitaries U_1 and U_2 with success probability $\geq 2/3$ given a promise on the diamond distance between U_1 and U_2.

Theorem 1 (Diamond-norm lower bound for unitary channel discrimination)**.** *Let $\theta \in [0, 2\pi)$ and let $U_1, U_2 \in \mathbb{U}(d)$ such that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$. Now let $U \in \{U_1, U_2^\theta\}$ with $U_2^\theta = e^{i\theta} U_2$ be a unitary to which one has black-box access, including controlled operations, applications of the inverse and a combination of both. Suppose one has to decide whether (i) $U = U_1$ or (ii) $U = U_2^\theta$ holds, promised that either one of them is the case and $\frac{1}{2} \left\| \mathcal{U}(U_1) - \mathcal{U}(U_2) \right\|_\diamond \leq \epsilon$. Then there exists a $\theta \in [0, 2\pi)$ such that to decide with success probability $\geq 2/3$ whether (i) or (ii) holds, any C-tester with $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$ needs to make at least*

$$T \geq \Omega\left(\frac{1}{\epsilon}\right)$$

queries to U.

Essentially, Theorem 1 establishes in a unitary query setting what is known as *Heisenberg-limited scaling* (or the *Heisenberg limit*) in quantum sensing and metrology [13, 14]. This implies that achieving a $1/N$-factor improvement in accuracy requires $\sim N$ additional "resources," which, in our case, correspond to queries. Since the Heisenberg limit is an information-theoretic notion, it should apply universally—including computational settings that allow (quantum) proofs and advice.

Variations of Theorem 1 were already proven in other works [8, 10], but to our knowledge not in the setting where (i) one considers access to quantum proofs and/or advice and (ii) a computational model which allows for access to the inverse, controlled and controlled inverse of U. Moreover, we would like to stress that the key contribution of this work is to give a unified exposition of the idea[2] that Theorem 1 can be used as a general framework to prove lower bounds for unitary property testing problems in the setting where one is given advice as well as proofs, by adopting the following strategy:

1. Given a unitary property $\mathcal{P} = (\mathcal{P}_{\mathrm{yes}}, \mathcal{P}_{\mathrm{no}})$, find two unitaries U_1, U_2 such that $U_1 \in \mathcal{P}_{\mathrm{yes}}$ and $U_2 \in \mathcal{P}_{\mathrm{no}}$.

2. Show that a unitary property tester for $\mathcal{P}$ implies a distinguisher for U_1 and U_2.

3. Prove a lower bound on the channel discrimination complexity of U_1, U_2 using Theorem 1, which implies a lower bound on the query complexity of the unitary property tester.

As we will show in the main body of the paper, this strategy turns out to be a powerful procedure to obtain simple, yet often tight lower bounds for a wide range of unitary property testing and related problems. For example, the lower bound of quantum phase estimation as proven by Bessen [15], relies on frequency analysis and takes up a 7-page

[2]Proving lower bounds by reducing the discrimination and identification tasks is a standard tool in theoretical computer science.

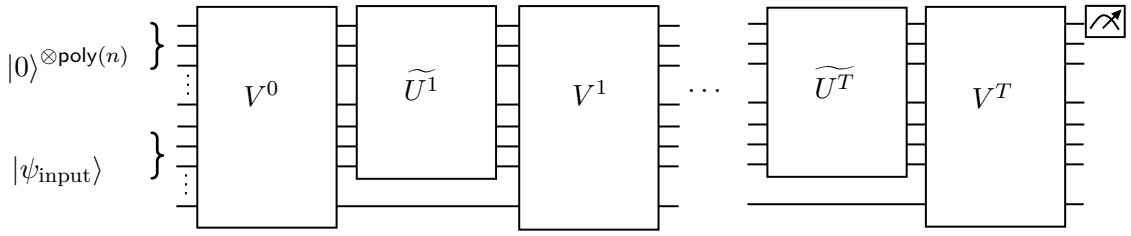

Figure 1: Query complexity model for unitary property tester making T queries to a unitary of interest U. The initial state is $|\psi_{\mathsf{init}}\rangle = |0\rangle^{\otimes \mathsf{poly}(n)} |\psi_{\mathsf{input}}\rangle$ is allowed to consist of an input-independent part and an input-dependent part, depending on the class C of the C-property tester. The unitary of interest U can be accessed directly, through its inverse, controlled or controlled inverse, i.e. we have that $\tilde{U}^t \in \{U_i, U_i^\dagger, cU_i, cU_i^\dagger\}$ for all $t \in [T]$, $i \in \{1, 2\}$.

double-column paper. Using our technique, an optimal lower bound in a stronger setting (including proofs and advice) can be shown using a proof of just 7 lines(!).[3]

1.2 Applications

We consider many of the same unitary property testing problems as in the work by Wang and Zhang [4], except for the *subset support verification* problem, which is a new problem we introduce in this work. Let us briefly sketch the definitions of all four unitary property testing problems considered:

- **Quantum phase estimation:** given access to a unitary U and an eigenstate $|\psi\rangle$, determine whether the eigenphase $\theta : U|\psi\rangle = e^{2i\pi\theta}|\psi\rangle$ satisfies $\theta \geq b$ or $\leq a$ for $b - a = \epsilon$.
- **Entanglement entropy:** given access to a bipartite state $|\psi\rangle_{AB} \in \mathbb{C}^d \otimes \mathbb{C}^d$ through a unitary $U = \mathbb{I} - |\psi\rangle\langle\psi|$, determine whether $S_2(\mathrm{tr}_B(|\psi\rangle\langle\psi|)) \leq a$ or $\geq b$ with $b - a = \Delta$, where $S_2(\rho) = -\ln[\mathrm{tr}[\rho^2]]$.
- **Subset support verification:** given access to a subset $S \subseteq \{0,1\}^n$ through a unitary $U : U|0^n\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$, determine whether $j \in S$ or $j \notin S$ for some string $j \in \{0,1\}^n$.
- **Quantum amplitude estimation:** given a unitary U which acts as $U|0^n\rangle = \sqrt{\alpha}|\psi\rangle + \sqrt{1-\alpha}|\psi^\perp\rangle$, determine whether $\sqrt{\alpha} \geq b$ or $\leq a$ with $b - a = \epsilon$.

Additionally, we also consider the following four unitary problems, which are not unitary property testing problems:

- **Thermal state preparation:** given access to some Hamiltonian H through a block-encoding U_H prepare (an approximation of) the Gibbs state $e^{-\beta H}/\mathrm{tr}\left[e^{-\beta H}\right]$ at inverse temperature β.
- **Hamiltonian simulation:** given access to some Hamiltonian H through a block-encoding U_H, implement (an approximation of) e^{itH} for some time t.
- **Hamiltonian learning:** given access to some Hamiltonian H via its time evolution operator $U(t) = e^{itH}$, output the matrix description of H in the computational basis, minimizing the total evolution time.

[3] Of course, this is a slight cheat in the way we count, but hopefully this captures the gist that this technique—once it is set up—is powerful in its simplicity.

- **Ground state preparation (GSP) of gapped Hamiltonians:** given access to some Hamiltonian H through a block-encoding U_H, implement (an approximation of) the ground state of H.

Problem	Query lower bound
Quantum phase estimation (Claim 1)	$\Omega\left(1/\epsilon\right)$
Entanglement entropy (Claim 2)	$\Omega\left(1/\sqrt{\Delta}\right)$
Subset support verification (Claim 3)	$\Omega\left(\sqrt{\lvert S\rvert}\right)$
Quantum amplitude estimation (Corollary 2)	$\Omega\left(1/\epsilon\right)$
Thermal state preparation (Claim 4)	$\Omega(\beta)$
Hamiltonian simulation (Claim 5)	$\Omega(t)$
Hamiltonian learning (Claim 6)	$\Omega(1/\epsilon)$
GSP of gapped Hamiltonians (Claim 7)	$\Omega(1/\Delta)$

Table 1: Obtained bounds for the query complexity of unitary property testing and related problems. All bounds hold for any C-tester with $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$ and are, with the exception of the entanglement entropy problem, shown to be tight (up to logarithmic factors) in Section 4.

Table 1 summarises our obtained bounds for the above problems. All our lower bounds are obtained via Theorem 1, and upper bounds are given by known results or explicitly proven in the main text (see Section 4). With the exceptions of subset support verification and entanglement entropy, these bounds were already known to hold in literature [15, 16, 17, 18, 19, 20, 21].[4] However, our work is (as far as the author is aware) the first to show that these bounds hold even in the presence of *both* (quantum) proofs and advice.[5]

1.3 Quantum oracle separations and implications to QMA(2)

One of the main takeaways of the results in Table 1 seems to be that whenever high precision is required in a black-box setting, neither quantum proofs nor advice seems to help in reducing the required query complexity. The complexity class $\mathsf{QMA}(k)$ is a generalisation of QMA where there are k multiple *uninteracting* provers, which are thus guaranteed to be unentangled with each other. It is known that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ for $2 \leq k \leq \mathsf{poly}(n)$ [22], but is generally believed that $\mathsf{QMA} \neq \mathsf{QMA}(2)$, since there are problems known to be in $\mathsf{QMA}(2)$ but not known to be in QMA [23, 24, 25, 26]. However, it is still a major open question of how more powerful $\mathsf{QMA}(2)$ can be—the best upper bound we currently have is $\mathsf{QMA}(2) \subseteq \mathsf{NEXP}$, which follows by just guessing exponential-size classical descriptions of the two quantum proofs. So could $\mathsf{QMA}(2)$ even be equal to NEXP, or even contain, say, PSPACE? In order for this to be true, it needs to at least contain the class SBQP in the unrelativized world, where $\mathsf{SBQP} \subseteq \mathsf{PP}$ can be viewed as a variant of BQP with exponentially close completeness and soundness parameters. However, our results easily imply a quantum oracle relative to which this is not true:

[4] The lower bound in Ref. [17] assumes sparse access to the entries of the local Hamiltonian, which is a stronger input model than the block-encoding setting we consider.

[5] Mande and de Wolf [19] also give a lower bound on quantum phase estimation with advice, but the advice in their work refers to something different: the problem they consider generalises quantum phase estimation in the sense that you are no longer given the exact eigenstate but only a quantum state, called an advice state, which has some promised *overlap* with it. In our case, advice refers to complexity classes that have access to some trusted string (or state) that may depend on the input length but not on the input itself.

Theorem 2. *There exists a quantum oracle U such that*

$$\mathsf{QMA}(2)^U \not\supset \mathsf{SBQP}^U.$$

The proof, given in Section 5, considers any unary language L that is not contained in either $\mathsf{QMA}(2)$ or SBQP, which must exist by a counting argument. We then encode $L(x)$ as an eigenphase corresponding to the eigenstate $|0\rangle$ in a diagonal unitary: the phase is 0 if $x \notin L$ and exponentially close to 0 if $x \in L$. Running a one-bit quantum phase estimation circuit [27] with this unitary then yields an exponentially small probability of measuring $|1\rangle$ on the first qubit only when the eigenphase is non-zero. Therefore, we have that L is contained in SBQP^U, as it can distinguish exponentially small differences in the eigenphase making only a single controlled query to U. For $\mathsf{QMA}(2)$, the quantum oracle behaves almost like the identity operator for large input sizes. Hence, in these cases, U can be replaced by the identity operator while preserving a sufficiently large completeness and soundness gap. This would contradict the assumption that we considered some $L \notin \mathsf{QMA}(2)$.

Whilst this oracle separation is straightforward once one has Theorem 1, we believe it has theoretical merit: it implies that if $\mathsf{QMA}(2)$ would be able to solve very precise problems, for example the local Hamiltonian problem at exponentially precise precision (which is PSPACE-complete [28]), it needs to be able to do so in a way that does not work in a quantum black-box setting.

Similarly, we can use the same idea to show a quantum oracle separation between $\mathsf{QMA/qpoly}$ and SBQP.[6]

Theorem 3. *There exists a quantum oracle U such that*

$$\mathsf{QMA/qpoly}^U \not\supset \mathsf{SBQP}^U.$$

1.4 Related work

Classical property testing in a quantum setting was first studied by Buhrman, Fortnow, Newman, and Hein Röhrig [30]. There are two main techniques for proving lower bounds on the quantum query complexity of classical property testing: the polynomial method [31] and the adversary method [32]. The methods are generally incomparable: there exist problems in which the polynomial method provides a tight lower bound and the adversary method provably not [33] and vice versa [34].[7]

The first study of unitary property testing by Wang [1] only includes upper bounds and raises the open question of finding a technique to show lower bounds for these kinds of problems.[8] In 2015 Belovs generalised the adversary method to include unitary property

[6] Contrary to what was claimed in an earlier version of this work, it is not clear if such an oracle separation holds if we consider both unentangled quantum proofs and advice, since we do not know whether $\mathsf{QMA}(2)/\mathsf{qpoly} = \mathsf{ALL}$ [29].

[7] This does not hold if one considers the negative weights (or generalized) adversary method [35], which is tight for every decision problem [36].

[8] The work also uses a more restricted query model: one starts with some arbitrary bipartite quantum state $|\psi_{AB}\rangle$, applies U (or its inverse) to the A-subsystem of $|\psi_{AB}\rangle$ followed by a measurement.

testing [37] and recently She and Yuen provided a lower bound method based on polynomials, which they also use to show lower bounds for QMA-testers [2]. Some other works that consider the query complexity of problems related to unitary property testing problems are Refs. [3, 19, 38, 39].

Comparison to Ref. [4]. We study many of the same problems as Wang and Zhang, but do so with a different technique: Wang and Zhang propose a sample-to-query lifting theorem, which translates a sample lower bound for any type of quantum state testing into a query lower bound for a corresponding type of unitary property testing. However, the obtained bounds using this method contain a sub-optimal inverse logarithmic factor, which seems to be inherent to their technique. The idea is to reduce unitary property testing problems to state discrimination, where the unitaries being tested block-encode the states from the state discrimination problem. The encoding consists of two steps: (1) copies of a state are used to approximately implement a quantum channel corresponding to time evolution under the density matrix as a Hamiltonian (known as density matrix exponentiation [40]), and (2) the density matrix exponentiation is leveraged within the quantum singular value transformation framework [41] to achieve a desired block-encoding (see Definition 8). Both steps are approximate, with the second incurring an additional logarithmic factor, leading to slightly suboptimal lower bounds. Moreover, their results are not shown to hold in the presence of quantum proofs and advice, which are two open problems raised in the discussion section of the paper. Using our technique we resolve both of these open problems for their obtained lower bounds.

1.5 Open questions

Can one improve either the upper or lower bound for the entanglement entropy problem, such that both bounds match?[9] Are there more unitary problems for which our method can prove (tight) lower bounds? Are there more examples of unitary property testing problems besides the quantum search problem from Ref. [7], where one can show that quantum proofs provably reduce the quantum query complexity? What about quantum advice?

Acknowledgements. JW thanks Harry Buhrman, Alvaro Yanguez and Marco Túlio Quintino for useful discussions, and Amira Abbas, Jonas Helsen, Ronald de Wolf and Sebastian Zur for comments on an earlier draft. Anonymous referees are also thanked for their feedback on earlier versions. JW was supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

2 Preliminaries

2.1 Notation

We write $[n]$ to denote the set of integers $\{1, 2, \ldots, n\}$. For a matrix M, we write $\mathrm{eig}(M)$ to denote the set of eigenvalues of M. For any $d \in \mathbb{N}$, $\mathbb{I}_d$ will be the d-dimensional identity matrix. If the dimension is clear from the context, we simply write $\mathbb{I}$. If X is a finite set, $|X|$ is the size of X and $\mathrm{conv}(X)$ the convex hull of the elements in X. We write

[9] Following this work, Chen, Wang and Zhang improved the lower bound for the entanglement entropy to $\tilde{\Omega}(d/\Delta)$, simultaneously a dependence on the dimensionality d as well as the precision Δ [42]. However, as far as the author is aware, it is still open whether this lower bound can be matched by an upper bound.

$\mathsf{poly}(n)$ to denote an arbitrarily polynomially-bounded function. We denote $\mathbb{U}(d)$ for the unitary group of degree d and $\mathcal{D}(d)$ for the set of all d-dimensional density matrices ρ (i.e. all complex d by d matrices that are PSD and have trace 1). The operator, trace and diamond norm are denoted $\|\cdot\|_{\text{op}}$, $\|\cdot\|_{\text{tr}}$ and $\|\cdot\|_{\diamond}$, respectively.

2.2 Classes of unitary property testers

We follow the conventions in the definitions by She and Yuen [2]. For a fixed number of qubits n, let $\mathcal{P}_{\text{yes}}$ and $\mathcal{P}_{\text{no}}$ (called the yes and no instances, respectively) be *disjoint* subsets of all n-qubit unitary operators.[10] A tester for a unitary problem $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ is a quantum algorithm which given query access to $U \in \mathcal{P}_{\text{yes}} \cap \mathcal{P}_{\text{no}})$ accepts with high probability when $U \in \mathcal{P}_{\text{yes}}$ and accepts with low probability when $U \in \mathcal{P}_{\text{no}}$. Hence, the tester can discriminate between the unitaries coming from the set of yes instances $\mathcal{P}_{\text{yes}}$ and those from $\mathcal{P}_{\text{no}}$. This is more general than the standard definition in the literature, where the no-instances are defined to be ϵ-far from the set of yes instances in terms of some distance measure (see for example Ref. [38]). However, for our purposes we only need the sets $\mathcal{P}_{\text{yes}}$ and $\mathcal{P}_{\text{no}}$ to be disjoint.

We can now build classes of testers similar to Ref. [2]. First, Let us start with the simplest class of testers, which do not use proofs or advice. W.l.o.g., one can always consider the input states to be pure since the acceptance probability of any mixed state is always upper bounded by a pure state via a convexity argument. The initial state of any quantum algorithm is always assumed to have some number of ancilla qubits all initialised in $|0\rangle$ and is sometimes supplied with an additional input state, depending on the class of tester considered.

Definition 1 (BQP-tester)**.** *Let $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ be a unitary property on n qubits. We say $\mathcal{P}$ has a BQP-tester if there exists a quantum algorithm such that the following holds:*

- *If $U \in \mathcal{P}_{\text{yes}}$, the quantum algorithm makes queries to U and accepts with probability $\geq 2/3$.*
- *If $U \in \mathcal{P}_{\text{no}}$, the quantum algorithm makes queries to U and accepts with probability $\leq 1/3$.*

Note that there is no restriction on the number of queries the tester makes to U, as this is the quantity being characterized. Nor is there any restriction on the amount of space or time used by the BQP-tester in this definition, which makes the "P" in "BQP-tester" somewhat awkward. Nonetheless, we adopt this notation to follow the convention in Ref. [2] and to facilitate a direct connection to separations between actual complexity classes (Section 5).

Let us now add, possibly unentangled, quantum (resp. classical) proofs to define QMA (resp. QCMA) testers.

Definition 2 ($\mathsf{QMA}(k)$-tester)**.** *Let $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ be a unitary property on n qubits. We say $\mathcal{P}$ has a $\mathsf{QMA}(k)$-tester if the following holds:*

- *If $U \in \mathcal{P}_{\text{yes}}$, then there exists k quantum states $\{|\xi_i\rangle\}$ such that on input $|\xi_1\rangle \dots |\xi_k\rangle$ the algorithm makes queries to U and accepts with probability $\geq 2/3$.*
- *If $U \in \mathcal{P}_{\text{no}}$, then for all k quantum states $\{|\xi_i\rangle\}$, the algorithm acting on $|\xi_1\rangle \dots |\xi_k\rangle$ makes queries to U and accepts with probability $\leq 1/3$.*

[10] More generally, one would consider all d-dimensional unitaries for an arbitrary dimension d.

If $k = 1$, we abbreviate to a QMA*-tester.*

Definition 2a (QCMA-tester)**.** *This has the same definition as the* QMA*-tester, but where the promises hold with respect to computational basis states $|y\rangle$ as input states.*

By the result of Harrow and Montanaro, it would suffice to consider QMA(2)-testers to cover all of QMA(poly(n)) [22].

The definitions of testers of unitary properties in Ref. [2] do not include classes which allow for advice. A technical difficulty that arises when one wants to include advice states is that we need to specify a notion of input length on which the advice may depend. in Ref. [2], no such restrictions were necessary, and all classes of testers were defined in a way that did not in any way depend on any notion of input size n. We will make the choice that n is given by the number of qubits the unitary acts on. Note that in the case where the property is also parametrised by some parameter, this is not restrictive in the advice setting since every parameter setting is a different unitary property and hence allows for a different choice of advice strings. To make this point clear, take the example of a unitary property testing formulation of quantum phase estimation with a variable number of qubits n but a fixed sequence of known eigenstates $|\psi_n\rangle$, for example $|0^n\rangle$: here one has to determine if an unknown n-qubit unitary U comes from $\mathcal{P}_{\text{yes}} = \{U : U|0^n\rangle = |0^n\rangle\}$ or $\mathcal{P}_{\text{no}} = \{U : U|0^n\rangle = e^{2\pi i\theta}|0^n\rangle, \epsilon \leq \theta \leq 1/2\}$ for some fixed $\epsilon > 0$. In other words, promised that U has an eigenstate $|\psi\rangle$, determine if its eigenphase is 0 or $\geq \epsilon$. In this case, one could also parametrise ϵ as a function of some m, i.e., $\epsilon = \epsilon(m)$. In this case, for a fixed choice of ϵ, the advice should be identical for each fixed n. However, even for fixed values of n, the advice can be different for different values of ϵ as each is a new property testing problem. Having set our choice of what the input size n means, we will now state our definitions of the testers.

Definition 3 (BQP/qpoly-tester)**.** *Let $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ be a unitary property on n qubits. We say $\mathcal{P}$ has a* BQP/qpoly*-tester if there exists a collection of quantum advice states $\{|\psi_n\rangle\}$, and a quantum algorithm such that the following holds:*

- *If $U \in \mathcal{P}_{\text{yes}}$, on input $|\psi_n\rangle$ the quantum algorithm makes queries to U and accepts with probability $\geq 2/3$.*
- *If $U \in \mathcal{P}_{\text{no}}$, on input $|\psi_n\rangle$ the quantum algorithm makes queries to U and accepts with probability $\leq 1/3$.*

Definition 3a (BQP/poly-tester)**.** *This has the same definition as the* BQP/qpoly*-tester but where the advice states are computational basis states $|y_n\rangle$.*

We can also combine proofs and advice to arrive at even more powerful classes of testers.

Definition 4 (QMA(k)/qpoly-tester)**.** *Let $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ be a unitary property on n qubits. We say $\mathcal{P}$ has a* QMA(k)/qpoly*-tester if there exists a collection of quantum advice states $\{|\psi_n\rangle\}$, where $|\psi_n\rangle \in (\mathbb{C}^2)^{\otimes \text{poly}(n)}$, and a quantum algorithm such that the following holds:*

- *If $U \in \mathcal{P}_{\text{yes}}$, then there exists k quantum states $\{|\xi_i\rangle\}$, such that on input $|\psi_n\rangle|\xi_1\rangle \ldots |\xi_k\rangle$ the algorithm makes queries to U and accepts with probability $\geq 2/3$.*
- *If $U \in \mathcal{P}_{\text{no}}$, then for all k quantum states $\{|\xi_i\rangle\}$, the algorithm acting on $|\psi_n\rangle|\xi_1\rangle \ldots |\xi_k\rangle$ makes queries to U and accepts with probability $\leq 1/3$.*

In this case it still holds that $\mathsf{QMA}(\mathsf{poly}(n))/\mathsf{qpoly} = \mathsf{QMA}(2)/\mathsf{qpoly}$, since the $\mathsf{QMA}(2) = \mathsf{QMA}(\mathsf{poly}(n))$ result of Ref. [22] relies on being able to boost the completeness parameter c to be close to 1, which can be done by error reduction (if there is an advice state which works, then one is allowed to use as many copies as one wants, since it still satisfies the criterion that it only depends on the size of the input). One can also define $\mathsf{QCMA}/\mathsf{qpoly}$-, $\mathsf{QCMA}/\mathsf{poly}$- and $\mathsf{QCMA}/\mathsf{poly}$- and $\mathsf{QMA}/\mathsf{poly}$-testers by modifying the promises such that they hold with respect to basis states on either the proof, the advice or both. All classes of testers discussed so far are contained in $\mathsf{QMA}(2)/\mathsf{qpoly}$.

There is one more class we would like to introduce, which is fundamentally different from all classes of testers discussed so far in the sense that it allows for an exponentially small gap between the completeness and soundness parameters.

Definition 5 (SBQP-tester)**.** *Let $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ be a unitary property on n qubits. We say $\mathcal{P}$ has a SBQP-tester if there exists a quantum algorithm and a polynomial $p(n)$ such that the following holds:*

- *If $U \in \mathcal{P}_{\text{yes}}$, the quantum algorithm makes queries to U and accepts with probability $\geq 2^{-p(n)}$.*
- *If $U \in \mathcal{P}_{\text{no}}$, the quantum algorithm makes queries to U and accepts with probability $\leq 2^{-p(n)-1}$.*

2.3 Quantum information

In this work, all quantum systems will be finite-dimensional. For two d-dimensional quantum states described by density operators $\rho_1, \rho_2 \in \mathcal{D}(d)$, the trace distance is given by

$$\frac{1}{2}\left\|\rho_1 - \rho_2\right\|_{\text{tr}} = \frac{1}{2}\,\text{tr}\left[\sqrt{(\rho_1 - \rho_2)^\dagger(\rho_1 - \rho_2)}\right]. \tag{1}$$

Equivalently, the trace distance can be defined in a variational form as

$$\frac{1}{2}\left\|\rho_1 - \rho_2\right\|_{\text{tr}} = \sup_{0 \leq P \leq \mathbb{I}} \text{tr}\left[P(\rho_1 - \rho_2)\right], \tag{2}$$

where P is a positive operator. Hence, the trace distance characterizes the largest possible bias with which one can distinguish between states ρ_1 and ρ_2. A quantum channel $\mathcal{E}$ is a completely positive trace-preserving map between two density operators $\rho_1 \in \mathcal{D}(d_1)$ and $\rho_1 \in \mathcal{D}(d_2)$, where the dimensions d_1 and d_2 do not have to be the same. A special type of quantum channel is a unitary channel, which is a channel which applies to a d-dimensional density matrix ρ a mapping

$$\mathcal{U}(U) : \rho \to U\rho U^\dagger, \tag{3}$$

for some unitary $U \in \mathbb{U}(d)$. Given a unitary $U \in \mathbb{U}(d)$, we will also write $\mathcal{U}(U)$ for the unitary channel implementing a specified U as per Eq. (3). The distance between two quantum channels can be characterized using the so-called diamond distance, which is induced by the diamond norm.

Definition 6 (Diamond distance for quantum channels)**.** *Let d_a, d_b be the dimensions of two finite-dimensional Hilbert spaces. The diamond-norm distance, denoted as $\frac{1}{2}\left\|\mathcal{E}_1 - \mathcal{E}_2\right\|_\diamond$, between two quantum channels $\mathcal{E}_1, \mathcal{E}_2 : \mathcal{D}(d_a) \to \mathcal{D}(d_b)$ is given by*

$$\frac{1}{2}\left\|\mathcal{E}_1 - \mathcal{E}_2\right\|_\diamond = \frac{1}{2}\max_{\text{tr}(\rho)=1, \rho \succeq 0} \left\|(\mathcal{E} \otimes \mathbb{I}_{d_a})(\rho) - (\mathcal{E}_2 \otimes \mathbb{I}_{d_a})(\rho)\right\|_{\text{tr}}.$$

If $\mathcal{E}_1$ and $\mathcal{E}_2$ are the corresponding channels of unitaries U_1 and U_2, respectively, then

$$\frac{1}{2}\left\|\mathcal{U}(U_1)-\mathcal{U}(U_2)\right\|_\diamond = \frac{1}{2}\max_{\mathrm{tr}(\rho)=1,\rho\succeq 0}\left\|U_1\rho U_1^\dagger - U_2\rho U_2^\dagger\right\|_{\mathrm{tr}}.$$

The diamond distance between two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ precisely characterises the one-shot distinguishability between the two channels, i.e. the success probability of correctly identifying a channel (when they are given with equal probability) is given by

$$p_{\mathrm{succ}} = \frac{1}{2}+\frac{1}{2}\left\|\mathcal{E}_1-\mathcal{E}_2\right\|_\diamond. \tag{4}$$

We will need the following two useful properties of the diamond distance, which can be found in (or easily derived from) Propositions 3.44 and 3.48 in Ref. [12].

Lemma 1 (Two properties of the diamond distance)**.** *Let $d_a, d_b, d_c \geq 1$ be arbitrary dimensions of the complex Hilbert spaces. The diamond distance satisfies the following two properties:*

1. *Unitary invariance. For all quantum channels $\mathcal{E}_1$,$\mathcal{E}_2 : \mathcal{D}(d_a) \to \mathcal{D}(d_b)$, for all $U \in \mathbb{U}(d_a)$ and $V \in \mathbb{U}(d_B)$ we have*

$$\left\|\mathcal{E}_1-\mathcal{E}_2\right\|_\diamond = \left\|\mathcal{E}_1'-\mathcal{E}_2'\right\|_\diamond,$$

   where $\mathcal{E}_i' = V\mathcal{E}_i(U\rho U^\dagger)V^\dagger$ for a $\rho \in \mathcal{D}(d_a)$, for $i \in \{1,2\}$.

2. *Hybrid argument. For all quantum channels $\mathcal{E}_1, \mathcal{E}_1' : \mathcal{D}(d_a) \to \mathcal{D}(d_b)$, $\mathcal{E}_2, \mathcal{E}_2' : \mathcal{D}(d_b) \to \mathcal{D}(d_c)$, we have that*

$$\left\|\mathcal{E}_1\mathcal{E}_2-\mathcal{E}_1'\mathcal{E}_2'\right\|_\diamond \leq + \left\|\mathcal{E}_1-\mathcal{E}_1'\right\|_\diamond + \left\|\mathcal{E}_2-\mathcal{E}_2'\right\|_\diamond.$$

3 Lower bounds by unitary channel discrimination

In this section we will prove Theorem 1. First, we will set up some more preliminaries regarding unitary channel discrimination. For unitary channels, the definition of diamond norm allows for a more easily computable expression, as shown in the following lemma.

Lemma 2 (Adapted from Ref. [11])**.** *Let $U_1, U_2 \in \mathbb{U}(d)$ such that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$. Then*

$$\frac{1}{2}\left\|\mathcal{U}(U_1)-\mathcal{U}(U_2)\right\|_\diamond = \sqrt{1-D^2}, \tag{5}$$

with

$$D = \frac{1}{2}\min_{k,l}\left|e^{i\theta_k}+e^{i\theta_l}\right| \tag{6}$$

where $e^{i\theta_k}, e^{i\theta_l} \in \mathrm{eig}(U_1^\dagger U_2)$.

The quantity D has a nice geometrical interpretation: if $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$, then it is precisely the distance between the convex hull of the eigenvalues of $U_1^\dagger U_2$ and the origin. To determine whether $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$, it is useful to consider the *spectral arc-length* of U, given by the following definition.

Definition 7 (Spectral arc-length)**.** *The spectral arc-length* $\Theta(U)$ *of a unitary* $U \in \mathbb{U}(d)$ *is given by the length of the shortest compact interval* $I \subset \mathbb{R}$ *such that the corresponding segment* e^{iI} *contains the spectrum of* U*.*

It is easy to show that $0 \notin \mathrm{conv}(\mathrm{eig}(U)$ if and only if $\Theta(U) < \pi$ [43] (see also Fig. 2).

There are more ways to characterise the diamond distance for unitaries, which might be more convenient for some choices of unitaries as we try to prove lower bounds later down the road. Since we are interested in the asymptotic scaling of our lower bounds, it will sometimes be convenient to use the (global-phase shifted) operator norm difference between the two unitaries, as it is equivalent to the diamond norm up to a (inverse) factor of (at most) two.

Lemma 3 ([Adapted from [44])**.** *Let* $U_1, U_2 \in \mathbb{U}(d)$ *be unitaries. Then we have that*

$$\frac{1}{2}\left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond \leq \min_\phi \left\|e^{i\phi}U_1 - U_2\right\|_{\mathrm{op}} \leq \left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond .$$

As Lemma 3 involves a minimisation over a global phase factor $e^{i\phi}$, using the vanilla operator norm distance between two unitaries U_1 and U_2 would also yield an upper bound. Moreover, one can also show that a sufficient upper bound in operator norm implies the condition that $0 \notin \mathrm{conv}(\mathrm{eig}(U)$ is immediately satisfied, as illustrated by the following lemma.

Lemma 4. *Let* $U_1, U_2 \in \mathbb{U}(d)$ *be unitaries for which* $\left\|U_1 - U_2\right\|_{\mathrm{op}} \leq 2\sin\left(\frac{\pi-\delta}{4}\right)$ *for some small* $0 < \delta < \pi$*. Then it holds that* $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$*. For* $\delta = 0.04$*, we have* $2\sin\left(\frac{\pi-\delta}{4}\right) = 1.4$*.*

Proof. By unitary invariance of the operator norm it must hold that

$$\left\|U_1 - U_2\right\|_{\mathrm{op}} = \left\|\mathbb{I} - U_1^\dagger U_2\right\|_{\mathrm{op}} = \max_{\theta_j : e^{i\theta_j} \in \mathrm{eig}(U_1^\dagger U_2)} \left|1 - e^{i\theta_j}\right|.$$

Since all $e^{i\theta_j}$ are points on the unit circle in the complex plane, we can assume w.l.o.g. that $\theta_j \in [0, 2\pi]$ for all $j \in [d]$. Thus, we get the condition

$$\max_{\theta_j : e^{i\theta_j} \in \mathrm{eig}(U_1^\dagger U_2)} 2\left|\sin\left(\frac{\theta_j}{2}\right)\right| \leq 2\sin\left(\frac{\pi-\delta}{4}\right),$$

which means that $0 \leq \theta_j \leq (\pi - \delta)/2$ or $2\pi - (\pi - \delta)/2 \leq \theta_j \leq 2\pi$ for all $j \in [d]$. Hence, all eigenvalues of $U_1^\dagger U_2$ must lie within the segment e^{iI} on the unit circle in the complex plane given by the bounded and closed interval $I = [-(\pi-\delta)/2, (\pi-\delta)/2]$, which has length $\pi - \delta$ and is compact by the Heine-Borel theorem. Therefore, Definition 7 combined with the assumption $0 < \delta < \pi$ implies that $\Theta(U_1^\dagger U_2) < \pi$, which means that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$. □

Now that we have established ways to evaluate the diamond distance between two unitaries, we will proceed by showing that adding a well-chosen global phase to one of the unitaries ensures that access to the inverse, controlled access, or a combination of both, does not increase the ability to discriminate between the two. To show this, first observe that the condition of 0 not being in the convex hull of the eigenvalues of $U_1^\dagger U_2$ is invariant to adding a global phase to one of the unitaries.

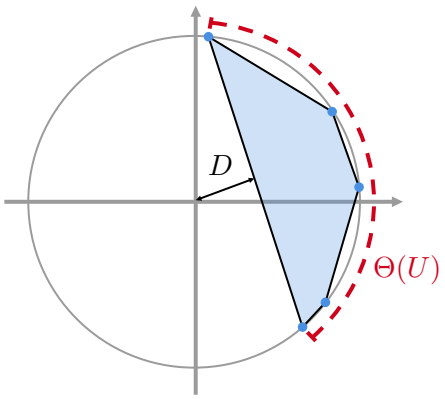

Figure 2: Geometrical interpretation in the complex plane of the spectrum of some $U \in \mathbb{U}(5)$. Since U is unitary, all its eigenvalues (blue dots) lie on the unit circle in the complex plane. Since the spectral arc-length (indicated by the red dashed line) satisfies $\Theta(U) < \pi$, we have that 0 is not in the convex hull of the eigenvalues of U (blue shaded area). The shortest distance from the origin to the convex hull of the spectrum of U is D.

Lemma 5. *Let $U_1, U_2 \in \mathbb{U}(d)$ such that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$. Let $U_2^\theta = e^{i\theta} U_2$. Then for all $\theta \in [0, 2\pi)$ we have $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2^\theta))$.*

Proof. This follows directly from the invariance of D under rotations, since $\mathrm{eig}(U_1^\dagger U_2^\theta) = \{e^{i\theta} e^{i\theta_l} | e^{i\theta_l} \in \mathrm{eig}(U_1^\dagger U_2)\}$ and

$$\frac{1}{2} \min_{k,l} \left| e^{i\theta} e^{i\theta_k} + e^{i\theta} e^{i\theta_l} \right| = \frac{1}{2} \min_{k,l} \left| e^{i\theta} \right| \left| e^{i\theta_k} + e^{i\theta_l} \right| = \frac{1}{2} \min_{k,l} \left| e^{i\theta_k} + e^{i\theta_l} \right|$$

for any $\theta \in [0, 2\pi)$. □

The next lemma proves the aforementioned claim that given some U_1, U_2 we can always pick a global phase such that the diamond distance between U_1 and U_2 precisely characterises the distance in the controlled, inverse, or controlled inverse setting.

Lemma 6 (Diamond distance for different query types)**.** *Let $U_1, U_2 \in \mathbb{U}(d)$ such that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$, and let $U_2^\theta = e^{i\theta} U_2$ for some $\theta \in [0, 2\pi)$. Then there exists a choice of θ such that for all choices $(\tilde{U}_1, \tilde{U}_2^\theta) \in \{(U_1, U_2^\theta), (U_1^\dagger, U_2^{\theta,\dagger}), (cU_1, cU_2^\theta), (cU_1^\dagger, cU_2^{\theta,\dagger})\}$ we have*

$$\frac{1}{2} \left\| \mathcal{U}(\tilde{U}_1) - \mathcal{U}(\tilde{U}_2^\theta) \right\|_\diamond = \frac{1}{2} \left\| \mathcal{U}(U_1) - \mathcal{U}(U_2^\theta) \right\|_\diamond .$$

Proof. By Lemma 5, we must have that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2^\theta))$ for any $\theta \in [0, 2\pi)$. We consider the separate cases using Lemma 2. The (U_1, U_2^θ)-case is trivially true.

Inverse queries. By Theorem 1.3.22 in Ref. [45] we have $\mathrm{eig}((U_1^\dagger)^\dagger U_2^{\theta,\dagger}) = \mathrm{eig}(U_2^{\theta,\dagger}(U_1^\dagger)^\dagger) = \mathrm{eig}((U_1^\dagger U_2^\theta)^\dagger)$. Therefore, for all $\theta \in [0, 2\pi)$ it holds that

$$\begin{aligned}\frac{1}{2}\left\|\mathcal{U}(U_1^\dagger) - \mathcal{U}(U_2^{\theta,\dagger})\right\|_\diamond &= \sqrt{1 - \left(\frac{1}{2}\min_{k,l}\left|e^{-i(\theta+\theta_k)} + e^{-i(\theta+\theta_l)}\right|\right)^2} \\ &= \sqrt{1 - \left(\frac{1}{2}\min_{k,l}\left|e^{i(\theta+\theta_k)} + e^{i(\theta+\theta_l)}\right|\right)^2} \\ &= \frac{1}{2}\left\|\mathcal{U}(U_1) - \mathcal{U}(U_2^\theta)\right\|_\diamond.\end{aligned}$$

Controlled queries. Note that we have that

$$\mathrm{eig}(cU_1^\dagger cU_2^\theta) = \mathrm{eig}(|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_1^\dagger U_2^\theta) = \mathrm{eig}(U_1^\dagger U_2^\theta) \cup \{1\}.$$

For all U_1, U_2 there exists a θ such that $1 \in \mathrm{eig}(U_1^\dagger U_2^\theta)$, simply by taking any eigenvalue $e^{i\theta_l} \in \mathrm{eig}(U_1^\dagger U_2)$ and letting $\theta = 2\pi - \theta_l$. Hence, for this choice of θ we have

$$\frac{1}{2}\left\|\mathcal{U}(cU_1) - \mathcal{U}(cU_2^\theta)\right\|_\diamond = \frac{1}{2}\left\|\mathcal{U}(U_1) - \mathcal{U}(U_2^\theta)\right\|_\diamond.$$

Controlled queries to the inverse. This follows directly by combining the two arguments above, and holds for the same values of θ. □

We restate Theorem 1 from Section 1 and give the proof.

Theorem 1 (Diamond-norm lower bound for unitary channel discrimination)**.** *Let $\theta \in [0, 2\pi)$ and let $U_1, U_2 \in \mathbb{U}(d)$ such that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$. Now let $U \in \{U_1, U_2^\theta\}$ with $U_2^\theta = e^{i\theta}U_2$ be a unitary to which one has black-box access, including controlled operations, applications of the inverse and a combination of both. Suppose one has to decide whether (i) $U = U_1$ or (ii) $U = U_2^\theta$ holds, promised that either one of them is the case and $\frac{1}{2}\left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond \leq \epsilon$. Then there exists a $\theta \in [0, 2\pi)$ such that to decide with success probability $\geq 2/3$ whether (i) or (ii) holds, any C-tester with $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$ needs to make at least*

$$T \geq \Omega\left(\frac{1}{\epsilon}\right)$$

queries to U.

Proof. We omit the dependence of θ in subsequent notation and assume that it is chosen according to Lemma 6. W.l.o.g. we can write the circuit $V^{U_i,(T)}$ which makes T queries to $\tilde{U}_i^{\,t} \in \{U_i, U_i^\dagger, cU_i, cU_i^\dagger,\}$, $i \in \{1, 2\}$, as

$$V^{U_i,(T)} = V_T \tilde{U}_i^T V_{T-1} \tilde{U}_i^{T-1} \dots V_1 \tilde{U}_i^1 V_0.$$

We want to measure a designated output qubit of $V^{U_i,(T)}$ in the computational basis, which should output 1 if we have U_1 and output 0 if we have U_2.

By Definition 6 and the operational interpretation of trace distance, we then have that for any input state $|\psi_{\text{init}}\rangle$

$$\left|\Pr\left[V^{U_1,(T)}(|\psi_{\text{init}}\rangle) \text{ outputs } 1\right] - \Pr\left[V^{U_2,(T)}(|\psi_{\text{init}}\rangle) \text{ outputs } 1\right]\right| \leq \frac{1}{2}\left\|\mathcal{U}(V^{U_1,(T)}) - \mathcal{U}(V^{U_2,(T)})\right\|_\diamond.$$

Let us show by induction on the number of queries that

$$\left\|\mathcal{U}(V^{U_1,(T)}) - \mathcal{U}(V^{U_2,(T)})\right\|_\diamond \leq 2T\epsilon.$$

For a single query, we have

$$\begin{aligned}
\left\|\mathcal{U}(V^{U_1,(1)}) - \mathcal{U}(V^{U_2,(1)})\right\|_\diamond &= \left\|\mathcal{U}(V_1\tilde{U}_1^1 V_0) - \mathcal{U}(V_1\tilde{U}_2^1 V_0)\right\|_\diamond && (7)\\
&= \left\|\mathcal{U}(\tilde{U}_1^1) - \mathcal{U}(\tilde{U}_2^1)\right\|_\diamond && (8)\\
&= \left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond && (9)\\
&\leq 2\epsilon, && (10)
\end{aligned}$$

using the unitary invariance of the diamond norm (Lemma 1, property 1) in going from line Eq. (7) to line Eq. (8) and Lemma 6 from going to line Eq. (8) to Eq. (9). For T queries, assuming the induction hypothesis on $T-1$ queries, we find

$$\begin{aligned}
\left\|\mathcal{U}(V^{U_1,(T)}) - \mathcal{U}(V^{U_2,(T)})\right\|_\diamond &= \left\|\mathcal{U}(V_T\tilde{U}_1^T V^{U_1,(T-1)}) - \mathcal{U}(V_T\tilde{U}_2^T V^{U_2,(T-1)})\right\|_\diamond && (11)\\
&\leq \left\|\mathcal{U}(V_T\tilde{U}_1^T) - \mathcal{U}(V_T\tilde{U}_2^T)\right\|_\diamond && (12)\\
&\quad + \left\|\mathcal{U}(V^{U_1,(T-1)}) - \mathcal{U}(V^{U_2,(T-1)})\right\|_\diamond\\
&\leq \left\|\mathcal{U}(V_T\tilde{U}_1^T) - \mathcal{U}(V_T\tilde{U}_2^T)\right\|_\diamond + 2(T-1)\epsilon && (13)\\
&= \left\|\mathcal{U}(\tilde{U}_1^T) - \mathcal{U}(\tilde{U}_2^T)\right\|_\diamond + 2(T-1)\epsilon && (14)\\
&= \left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond + 2(T-1)\epsilon && (15)\\
&\leq 2T\epsilon, && (16)
\end{aligned}$$

where the bound holds for any $|\psi_{\text{init}}\rangle$. Here we used Lemma 1, property 2, in going Eq. (11) to Eq. (12), the induction hypothesis in going from Eq. (12) to Eq. (13), the unitary invariance of the diamond norm from Eq. (13) to Eq. (14) and Lemma 6 from Eq. (14) to Eq. (15). Therefore, in order to have

$$\left|\Pr\left[V^{U_1,(T)}(|\psi_{\text{init}}\rangle) \text{ outputs } 1\right] - \Pr\left[V^{U_2,(T)}(|\psi_{\text{init}}\rangle) \text{ outputs } 1\right]\right| \geq \frac{2}{3} - \frac{1}{3} = \frac{1}{3},$$

we require

$$\frac{1}{3} \leq \frac{1}{3}\left\|\mathcal{U}(V^{U_1,(T)}) - \mathcal{U}(V^{U_2,(T)})\right\|_\diamond \leq T\epsilon,$$

which implies

$$T \geq \frac{1}{3\epsilon}. \tag{17}$$

We now have to show that Eq. (17) holds for $\mathsf{QMA}(2)/\mathsf{qpoly}$-testers. Let $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{yes}})$, where $\mathcal{P}_{\text{yes}} = \{U_1^1, U_1^2, \dots\}$ and $\mathcal{P}_{\text{no}} = \{U_2^1, U_2^2, \dots\}$, such that for each $n \in \mathbb{N}$ we have $\frac{1}{2}\left\|\mathcal{U}(U_1^n) - \mathcal{U}(U_2^n)\right\|_\diamond \leq \frac{1}{3T}$. Now suppose the above corollary is false, then there must exist an input quantum state $|\psi_{\text{input}}\rangle = |\psi_n\rangle|\xi_1\rangle\dots|\xi_k\rangle$ such that a T'-query quantum algorithm, $T' < T$, starting in the initial state $|\psi_{\text{init}}\rangle = |0\rangle^{\otimes \mathsf{poly}(n)}|\psi_{\text{input}}\rangle$, which makes queries to U can decide with probability $> 2/3$ whether $U \in \mathcal{P}_{\text{yes}}$ or $U \in \mathcal{P}_{\text{no}}$ (in the no-case the soundness property holds for all states, so also the one that is used in the yes-case). This contradicts the bound of Eq. (17), which holds for any $|\psi_{\text{init}}\rangle$. □

Remark 1. *Theorem 1 also holds when we replace the diamond norm condition on U_1 and U_2 by*

$$\min_{\phi} \left\| e^{i\phi} U_1 - U_2 \right\|_{\mathrm{op}} \leq \|U_1 - U_2\|_{\mathrm{op}} \leq \epsilon, \tag{18}$$

since we show that

$$\left\| \mathcal{U}(V^{U_1}) - \mathcal{U}(V^{U_2}) \right\|_{\diamond} \leq T \left\| \mathcal{U}(U_1) - \mathcal{U}(U_2) \right\|_{\diamond},$$

where

$$\frac{1}{2} \left\| \mathcal{U}(U_1) - \mathcal{U}(U_2) \right\|_{\diamond} \leq \min_{\phi} \left\| e^{i\phi} U_1 - U_2 \right\|_{\mathrm{op}},$$

by Lemma 3.

With Theorem 1 in hand, our proposed lower bound technique is now straightforward: given a unitary property $\mathcal{P} = (\mathcal{P}_{\mathrm{yes}}, \mathcal{P}_{\mathrm{no}})$, one picks two unitaries U_1, U_2 such that $U_1 \in \mathcal{P}_{\mathrm{yes}}$ and $U_2 \in \mathcal{P}_{\mathrm{no}}$; this implies that any unitary property tester for $\mathcal{P}$ implies a distinguisher for U_1 and U_2. One evaluates the diamond distance (or an upper bound thereof) between U_1 and U_2 using Lemmas 2 and 3 or any other suitable method, and verifies the property of $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2))$, possibly with the help of Lemma 5. The lower bound on the channel discrimination query complexity of U_1, U_2 follows then from Theorem 1, which directly implies a lower bound on the query complexity of the unitary property tester.

4 Applications

In this section we will apply the lower bound method of Section 3 to some problems in unitary property testing as well as some other unitary problems, showcasing the fact that the technique is very simple to use and (for all but one problem) leads to optimal lower bounds.

4.1 Unitary property testing

4.1.1 Quantum phase estimation

In quantum phase estimation, one is given a unitary U and an eigenstate $|\psi\rangle$, and the task is to determine the eigenphase of U corresponding to $|\psi\rangle$ up to some precision ϵ with probability $\geq 2/3$. A lower bound can be obtained by reducing the quantum counting problem to the amplitude estimation problem, which is then reduced to the phase estimation problem. From this, the lower bound of $\Omega(1/\epsilon)$ follows from the lower bound for quantum counting given in Ref. [16]. However, our method allows us to prove the same lower bound in only a couple of lines, and shows that it holds even in the presence of proofs and advice.

Claim 1 (Lower bound for quantum phase estimation)**.** *Let $U \in \mathbb{U}(d)$ and $|\psi\rangle$ a quantum state such that $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$, for some $\theta \in [0,1)$. Suppose that either (i) $\theta \geq b$ or (ii) $\theta \leq a$, with $b - a = \epsilon$. Then any C-tester, where $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$, that decides whether (i) or (ii) holds with probability $\geq 2/3$ has to make at least*

$$\Omega(1/\epsilon)$$

(controlled) queries to U (or its inverse).

Proof. Let $U_1 = \mathbb{I}$ and $U_2 = e^{2i\pi\epsilon}|0\rangle\langle 0| + |1\rangle\langle 1|$, with $\epsilon > 0$. Note $|\psi\rangle = |0\rangle$ is an eigenstate of both U_1 and U_2 with eigenphases $\theta_1 = 0$ and $\theta_2 = \epsilon$, respectively. Hence, any algorithm that decides whether some U with eigenstate $|\psi\rangle$ has an eigenphase $\theta \leq a := 0$ or $\geq b := \epsilon$ can discriminate U_1 from U_2. We have $\mathrm{eig}(U_1^\dagger U_2) = \{e^{2i\pi\epsilon}, 1\}$, which means $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2)$. Using $D = \frac{1}{2}|1 + e^{2i\pi\epsilon}|$ we find

$$\frac{1}{2}\left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond = \sqrt{1 - \frac{1}{4}|1 + e^{2i\pi\epsilon}|^2} = |\sin(\pi\epsilon)| \leq \pi\epsilon$$

for $\epsilon > 0$. Hence, by Theorem 1 we find $T \geq \Omega\left(1/\epsilon\right)$. □

This matches the well-known upper bound by Kitaev [27].

4.1.2 Entanglement entropy

In the entanglement entropy problem, one wants to decide whether a certain bipartite state $|\psi\rangle_{AB}$ has low or small entanglement entropy between the subsystems A and B. We consider the the (2-Rényi) entanglement entropy $S_2(\cdot)$, which for a mixed state ρ_A is defined as

$$S_2(\rho_A) = -\ln[\mathrm{tr}\left[\rho_A^2\right]].$$

Claim 2 (Lower bound for entanglement entropy)**.** *Let $U = \mathbb{I} - 2|\psi\rangle\langle\psi|$ be a unitary for some bipartite quantum state $|\psi\rangle = |\psi\rangle_{AB} \in \mathbb{C}^d \otimes \mathbb{C}^d$. Suppose that either (i) $S_2(\mathrm{tr}_B(|\psi\rangle\langle\psi|)) \leq a$ or (ii) $S_2(\mathrm{tr}_B(|\psi\rangle\langle\psi|)) \geq b$ with $b - a \geq \Delta$. Then any C-tester, where $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$, that decides whether (i) or (ii) holds with probability $\geq 2/3$ has to make at least*

$$T \geq \Omega\left(\frac{1}{\sqrt{\Delta}}\right)$$

(controlled) queries to U (or its inverse).

Proof. We reduce from the following unitary channel discrimination problem: $U_i = \mathbb{I} - 2|\psi_i\rangle\langle\psi_i|$, $i \in [1, 2]$, with

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle), \quad |\psi_2\rangle = \sqrt{\frac{1+\sqrt{\Delta}}{2}}|00\rangle + \sqrt{\frac{1-\sqrt{\Delta}}{2}}|11\rangle \tag{19}$$

We have

$$\rho_{1,A} = \mathrm{tr}_B[|\psi_1\rangle\langle\psi_1|] = I_2$$

which has $S_2(\rho_{1,A}) = \ln(2)$ and

$$\rho_{2,A} = \mathrm{tr}_B[|\psi_2\rangle\langle\psi_2|] = \frac{1+\sqrt{\Delta}}{2}|0\rangle\langle 0| + \frac{1-\sqrt{\Delta}}{2}|1\rangle\langle 1|$$

which has $S_2(\rho_{2,A}) = -\ln((1+\Delta)/2) \leq \ln(2) - \Delta/2$, so $b - a \geq \Delta/2$. Hence, if we could compute $S_2(\rho_i)$ up to precision $< \Delta/4$ for $i \in \{1, 2\}$ given access to U_i we could distinguish U_1 from U_2. We have that

$$\mathrm{eig}(U_1^\dagger U_2) = \{1, -i\sqrt{\Delta} + \sqrt{1-\Delta}, i\sqrt{\Delta} + \sqrt{1-\Delta}\},$$

which means that $0 \notin \text{conv}(\text{eig}(U_1^\dagger U_2)$ for $\Delta < 1$. We can brute force over all combinations of eigenvalues to find $D = \sqrt{1-\Delta}$ and thus

$$\frac{1}{2}\left\|\mathcal{U}(U_1) - \mathcal{U}(U_2)\right\|_\diamond = \sqrt{1-(1-\Delta)} = \sqrt{\Delta}$$

for $\Delta > 0$. By Theorem 1, we find a lower bound of $T \geq \Omega(1/\sqrt{\Delta})$. □

This removes the logarithmic factor of $\tilde{\Omega}(1/\sqrt{\Delta})$ in Ref. [4], and also resolves their open question whether their bound could be made to hold for a QMA-tester (we show in fact that it is robust against even stronger classes of testers). From the proof of Claim 2 it is easy to show that the following corollary holds:

Corollary 1. *The same lower bound applies when given copies of $|\psi\rangle$ instead of the unitary $U = \mathbb{I} - 2|\psi\rangle\langle\psi|$ from Claim 2.*

Proof. We consider the same states as in the proof of Claim 2. We can write $|00\rangle$ in terms of the two-dimensional subspace $\{|\psi_2\rangle, \left|\psi_2^\perp\right\rangle\}$ as

$$|00\rangle = \sqrt{\frac{1+\sqrt{\Delta}}{2}}|\psi_2\rangle + \sqrt{\frac{1-\sqrt{\Delta}}{2}}\left|\psi_2^\perp\right\rangle.$$

Consider the circuit which applies $U_2 = \mathbb{I} - 2|\psi_2\rangle\langle\psi_2|$ to $|00\rangle$ controlled by a qubit in $|+\rangle$ and then measures this first qubit in the Hadamard basis. We have

$$\begin{aligned} cU_2|+\rangle|00\rangle = {} & \frac{1}{\sqrt{2}}|0\rangle\left(\sqrt{\frac{1+\sqrt{\Delta}}{2}}|\psi_2\rangle + \sqrt{\frac{1-\sqrt{\Delta}}{2}}\left|\psi_2^\perp\right\rangle\right) + \\ & \frac{1}{\sqrt{2}}|1\rangle\left(-\sqrt{\frac{1+\sqrt{\Delta}}{2}}|\psi_2\rangle + \sqrt{\frac{1-\sqrt{\Delta}}{2}}\left|\psi_2^\perp\right\rangle\right) \\ = {} & \sqrt{\frac{1+\sqrt{\Delta}}{2}}|-\rangle|\psi_2\rangle + \sqrt{\frac{1-\sqrt{\Delta}}{2}}|+\rangle\left|\psi_2^\perp\right\rangle \end{aligned}$$

which yields the state $|-\rangle|\psi_2\rangle$ when the measurement outcome is $|-\rangle$, which happens with probability $(1+\sqrt{\Delta})/2 \geq \frac{1}{2}$. For $|\psi_1\rangle$ the same bound holds since this is the case where $\Delta = 0$. Therefore, with an expected number of $\mathcal{O}(T')$ runs of the circuit T' copies can be created. Hence, by Markov's inequality, we have that there exists a quantum algorithm that creates T' copies of $|\psi_i\rangle$ with probability $1-\delta$, making only $\mathcal{O}(T'/\delta)$ queries to U_i. Hence, if we could solve the problem with high success probability using $o(T')$ copies, this would contradict the lower bound of Claim 2. □

A standard quantum in the literature to estimate the entanglement entropy, usually considered in the setting where the input to the state is given in a sample setting, is through the use of the SWAP-test [46]. This gives an upper bound on the query complexity in terms of the precision Δ, the dimension d, and an upper bound on the entanglement entropy S_{upper}.

Proposition 1. *Let $d = 2^n$ for some $n \in \mathbb{N}$, and $b, a \in [0, \ln(d)]$ with $b - a = \Delta > 0$. Suppose that we are given a number $S_{\text{upper}} \in [0, \log d]$, and access to a bipartite state*

$|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ *via a unitary* $U = \mathbb{I} - 2|\psi\rangle\langle\psi|$*, for which* $S_2(|\psi\rangle) \leq S_{\text{upper}}$ *holds. Then there exists a quantum algorithm that solves the entanglement entropy problem using*

$$\mathcal{O}\left(\frac{\sqrt{d}e^{S_{\text{upper}}}}{\Delta}\right)$$

queries to U*, with probability* $\geq 2/3$*.*

Proof. Let $\mathcal{A}$ be the quantum circuit which creates the maximally entangled state from the all-zeros state, i.e.

$$\mathcal{A}|0\ldots0\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle|j\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|\psi_j\rangle\left|\bar{\psi}_j\right\rangle,$$

using the fact that the maximally entangled state can be written in any orthonormal basis. By using exact amplitude amplification, we can prepare $|\psi\rangle$ exactly with probability 1 using $\mathcal{O}(\sqrt{d})$ queries to U and $\mathcal{A}$ [47]. Let $\mathcal{B}$ be the algorithm which does this. If the SWAP-test [48] is applied to two copies of a mixed state ρ, the probability of measuring 0 on the first qubit is given by $\frac{1}{2} + \frac{1}{2}\operatorname{tr}[\rho^2]$ (a proof of this can be found in Ref. [49]). Using the SWAP test in conjunction with quantum amplitude estimation [50], we can estimate $\operatorname{tr}[\rho_A^2]$ up to additive precision ϵ using $\mathcal{O}(1/\epsilon)$ copies of $|\psi\rangle$ (i.e., calls to $\mathcal{B}$) with high probability. To make the estimation, when it succeeds, biased towards always returning an overestimate, we can apply the simple trick of providing an estimate $\bar{x}$ up to $\epsilon/2$ additive precision and making our new estimate $\hat{x} := \bar{x} + \epsilon/2$. Let $x := \operatorname{tr}[\rho_A^2]$. If we are guaranteed an upper bound on the entanglement entropy of S_{upper}, then we have that $x \in [e^{-S_{\text{upper}}}, 1]$. Choosing $\epsilon = \Delta e^{-S_{\text{upper}}}$, we have

$$\begin{aligned}
|-\ln x - (-\ln \hat{x})| &= |-\ln(x+\epsilon) - (-\ln(x))| \\
&= \left|\ln\left(\frac{x}{x+\epsilon}\right)\right| \\
&= \ln(1+\epsilon/x) \\
&\leq \ln\left(1+\epsilon e^{S_{\text{upper}}}\right) \\
&\leq \epsilon e^{S_{\text{upper}}} \\
&\leq \Delta/4,
\end{aligned}$$

which is a sufficient precision to distinguish between the two cases. Hence, we need to make a total of

$$T = \mathcal{O}\left(\sqrt{d}\cdot\frac{1}{\epsilon}\right) = \mathcal{O}\left(\frac{\sqrt{d}e^{S_{\text{upper}}}}{\Delta}\right)$$

queries to U. □

Our lower bound does not incorporate the dependence on the dimension, nor does it account for the fact that the estimation might become harder as the entanglement entropy approaches its maximum value. The lack of dimension-dependence might be explained by the fact that our lower bound does not take into account the difficulty of preparing $|\psi\rangle$ given access to U_i, as indicated by Corollary 1.

However, even when S_{upper} and d are constant, this bound is still quadratically worse in the precision Δ than the lower bounds from Claim 2 and Ref. [4]. We leave it as an open question whether these bounds (upper or lower) can be improved, especially in terms of achieving a better dependency on the precision Δ.

4.1.3 Subset support verification and amplitude estimation

Here we consider a variant to the amplitude estimation problem, which we will call the *subset support verification* problem. In this problem, one is given access to a unitary U which prepares a subset state for some subset $S \subseteq \{0,1\}^n$ when applied to the all-zeros state, as well as a bit string $j \in \{0,1\}^n$. The task is to decide whether $j \in S$ or $j \notin S$.

Claim 3 (Lower bound for subset support verification)**.** *Let U be a unitary that applies a transformation of the form*

$$U\left|0^n\right\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle ,$$

and let $j \in \{0,1\}^n$. Then any C-tester, where $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$, that decides whether $j \in S$ or $j \notin S$ with probability $\geq 2/3$ has to make at least

$$T \geq \Omega\left(\sqrt{|S|}\right)$$

(controlled) queries to U (or its inverse).

Proof. Let $S \subseteq \{0,1\}^n$ be any subset that contains 0^n, and let $j = 0^n$ (the proof can easily be modified to work for any choice of j). We can construct an explicit unitary U by setting $U = 2\left|v\right\rangle\!\left\langle v\right| - \mathbb{I}$, where

$$\left(2\left|v\right\rangle\!\left\langle v\right| - \mathbb{I}\right)\left|0^n\right\rangle = \left|S\right\rangle .$$

Solving for $|v\rangle$, using that $\langle 0 \ldots 0|S\rangle$ is real we obtain

$$|v\rangle = \frac{|0^n\rangle + |S\rangle}{\sqrt{2(1 + \langle 0 \ldots 0|S\rangle)}}.$$

Let $S_1 = S$ and $S_2 = S_1 \setminus \{0^n\}$. We define

$$|v_1\rangle = \frac{|0^n\rangle + |S_1\rangle}{\sqrt{2(1 + \sqrt{1/|S|})}}, \quad |v_2\rangle = \frac{|0^n\rangle + |S_2\rangle}{\sqrt{2}},$$

and

$$U_1 = 2\left|v_1\right\rangle\!\left\langle v_1\right| - \mathbb{I}, \quad U_2 = 2\left|v_2\right\rangle\!\left\langle v_2\right| - \mathbb{I}.$$

We can write $|v_2\rangle = \sqrt{1-\alpha}\,|v_1\rangle + \sqrt{\alpha}|v_1^{\perp}\rangle$ for some $\alpha \in [0,1]$. We have

$$U_2 = 2\left[(1-\alpha)\left|v_1\right\rangle\!\left\langle v_1\right| + \sqrt{1-\alpha}\sqrt{\alpha}\left|v_1\right\rangle\left\langle v_1^{\perp}\right| + \sqrt{1-\alpha}\sqrt{\alpha}\left|v_1\right\rangle\!\left\langle v_1^{\perp}\right| + \alpha\left|v_1^{\perp}\right\rangle\!\left\langle v_1^{\perp}\right|\right] - \mathbb{I}.$$

Writing $U_1^{\dagger}U_2$ in the $\{|v_1\rangle, \left|v_1^{\perp}\right\rangle, \ldots\}$ basis we obtain

$$U_1^{\dagger}U_2 = \begin{bmatrix} B & 0 \\ 0 & I_{2^{n-1}} \end{bmatrix},$$

where B is a 2×2-matrix given by

$$B = \begin{bmatrix} 1-2\alpha & 2\sqrt{1-\alpha}\sqrt{\alpha} \\ -2\sqrt{1-\alpha}\sqrt{\alpha} & 1-2\alpha \end{bmatrix}.$$

Since $U_1^\dagger U_2$ is a block-diagonal matrix, its eigenvalues are given by

$$\mathrm{eig}(U_1^\dagger U_2) = \mathrm{eig}(B) \cup \mathrm{eig}(\mathbb{I}_{2^{n-1}}) = \{1, 1-2\alpha-2\sqrt{\alpha^2-\alpha}, 1-2\alpha+2\sqrt{\alpha^2-\alpha}\}.$$

Again, it is easy to see that for $\alpha < 1$ we have $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U_2)$. Therefore, $D = 1-2\alpha$ and

$$\frac{1}{2}\left\|(\mathcal{U}(U_1) - \mathcal{U}(U_2))\right\|_\diamond = 2\sqrt{\alpha-\alpha^2} \leq 2\sqrt{\alpha} \leq 2\sqrt{\frac{1}{|S|}}$$

since,

$$\begin{aligned}
\sqrt{\alpha} &= \sqrt{1-|\langle v_1|v_2\rangle|^2} \\
&= \sqrt{1-\left|\frac{1+\langle 0^n|S_2\rangle+\langle S_1|0^n\rangle+\langle S_1|S_2\rangle}{2\sqrt{1+\sqrt{1/|S|}}}\right|^2} \\
&= \sqrt{1-\left|\frac{1+\sqrt{1/|S|}+\sqrt{(|S|-1)/|S|}}{2\sqrt{1+\sqrt{1/|S|}}}\right|^2} \\
&= \sqrt{\frac{1}{2}-\frac{1}{2}\sqrt{\frac{|S|-1}{|S|}}} \\
&\leq \sqrt{\frac{1}{2}-\frac{1}{2}\frac{|S|-1}{|S|}} \\
&\leq \sqrt{\frac{1}{|S|}}.
\end{aligned}$$

Hence, by Theorem 1 we have that $T \geq \mathcal{O}\left(\sqrt{|S|}\right)$ to distinguish U_1 and U_2 with probability $\geq 2/3$. □

The upper bound of $\mathcal{O}(\sqrt{S})$ follows directly from quantum amplitude estimation [50], for which the optimality is also a corollary of Claim 3, as it proves a lower bound in a more restricted setting.

Corollary 2 (Quantum amplitude estimation lower bound)**.** *Given a unitary U which acts as $U|0^n\rangle = \sqrt{\alpha}|\psi\rangle + \sqrt{1-\alpha}|\psi^\perp\rangle$. Suppose that either (i) $\sqrt{\alpha} \leq a$ or (ii) $\sqrt{\alpha} \geq b$ with $b - a = \epsilon$. Then any C-tester, where $\mathsf{C} \subseteq \mathsf{QMA}(2)/\mathsf{qpoly}$, that decides whether (i) or (ii) holds with probability $\geq 2/3$ has to make at least*

$$T \geq \Omega\left(\frac{1}{\epsilon}\right)$$

(controlled) queries to U (or its inverse).

Proof. Let $|S\rangle = \frac{1}{\sqrt{|S|}}\sum_{i\in S}|i\rangle$ with $|S| = 1/\epsilon^2$, where ϵ is chosen such that $|S|$ is integer (this assumption does not change the bound qualitatively). Let $|\psi\rangle = |0^n\rangle$. Note that

$$\sqrt{\alpha_1} = \langle 0^n|U_1|0^n\rangle = 1/\sqrt{|S|}, \quad \sqrt{\alpha_2} = \langle 0^n|U_2|0^n\rangle = 0,$$

so deciding whether $\sqrt{\alpha_i} = \frac{1}{\sqrt{|S|}} = \epsilon$ or $\sqrt{\alpha_i} = 0$ is sufficient to distinguish U_1 from U_2. By the proof of Claim 3, we then find $T \geq \Omega(1/\epsilon)$, completing the proof. □

4.2 Other unitary problems

The next two examples are not unitary property testing cases, but quantum algorithmic primitives involving the implementation of some unitary given access to some building block in the form of a *block-encoding* [51, 52].

Definition 8 (Block-encoding)**.** *Let M be $2^n \times 2^n$-dimensional matrix, $\alpha, \epsilon > 0$ and $a \in \mathbb{N}$. An $(n+a)$-qubit unitary operator U is an (α, a, ϵ)-block-encoding of M if*

$$\left\| \alpha(\langle 0|^{\otimes a} \otimes \mathbb{I}) U (|0\rangle^{\otimes a} \otimes \mathbb{I}) - M \right\|_{\text{op}} \leq \epsilon.$$

If $\alpha = a = 1$ and $\epsilon = 0$, we simply say that U is a block-encoding of M.

Given some n-qubit operator M, one can construct a $n+1$-qubit unitary operator U provided all singular values of M are upper bounded by 1 in the following way. Let $M = R\Sigma V^\dagger$ be the singular value decomposition (SVD) of M. Then

$$U = \begin{pmatrix} M & R\sqrt{\mathbb{I} - \Sigma^2}V^\dagger \\ R\sqrt{\mathbb{I} - \Sigma^2}V^\dagger & -M \end{pmatrix} \tag{20}$$

is a $(1, 1, 0)$-block-encoding of M, since

$$(\langle 0| \otimes I_2) U (|0\rangle \otimes I_2) = M.$$

4.2.1 Thermal state preparation (quantum Gibbs sampling)

For some Hamiltonian H, the thermal state ρ_β at inverse temperature β is defined as

$$\rho_\beta = \frac{e^{-\beta H}}{\text{tr}[e^{-\beta H}]}. \tag{21}$$

We say a quantum algorithm is an *approximate Gibbs sampler* if it prepares the thermal state ρ_β up to some trace distance ϵ. In Ref. [18], an optimal lower bound in β is proven in Appendix G. We demonstrate that this bound can also be derived using our framework. The main distinction is that we prove the result by directly examining the diamond distance between the block-encodings of the Hamiltonians, rather than using reflections about a purified Gibbs state.

Claim 4 (Lower bound for quantum Gibbs sampling)**.** *Let H be some Hamiltonian to which we have access through a block-encoding U_H. Suppose $\beta \geq \sqrt{\frac{14}{3}} \approx 2.16$. Then it takes at least*

$$T \geq \Omega(\beta)$$

queries to U_H to prepare the thermal state at inverse temperature β up to trace distance $\leq \frac{1}{24}$.

Proof. Let $H_1 = \left(\frac{1}{2} + \frac{1}{\beta}\right)|0\rangle\langle 0| + \left(\frac{1}{2} - \frac{1}{\beta}\right)|1\rangle\langle 1|$, and $H_2 = \left(\frac{1}{2} - \frac{1}{\beta}\right)|0\rangle\langle 0| + \left(\frac{1}{2} + \frac{1}{\beta}\right)|1\rangle\langle 1|$. We have that by Eq. (21) the thermal states are given by

$$\rho_{1,\beta} = \frac{1}{1+e^2}\begin{bmatrix} 1 & 0 \\ 0 & e^2 \end{bmatrix}$$

and

$$\rho_{2,\beta} = \frac{1}{1+e^2}\begin{bmatrix} e^2 & 0 \\ 0 & 1. \end{bmatrix}$$

Therefore,

$$\frac{1}{2}\left\|\rho_{1,\beta} - \rho_{2,\beta}\right\|_{\mathrm{tr}} = 1 - \frac{2}{1+e^2} \geq \frac{3}{4}.$$

Now suppose that we can only prepare some $\tilde{\rho}_{i,\beta}$ such that $\frac{1}{2}\left\|\tilde{\rho}_{i,\beta} - \rho_{i,\beta}\right\|_{\mathrm{tr}} \leq \epsilon$ for $i \in \{1,2\}$. By applying the reverse triangle inequality twice, we find that

$$\begin{aligned}
\frac{1}{2}\left\|\tilde{\rho}_{1,\beta} - \tilde{\rho}_{2,\beta}\right\|_{\mathrm{tr}} &= \frac{1}{2}\left\|\rho_{1,\beta} - \rho_{2,\beta} - (\rho_{1,\beta} - \tilde{\rho}_{1,\beta}) - (\tilde{\rho}_{2,\beta} - \rho_{2,\beta})\right\|_{\mathrm{tr}} \\
&\geq \frac{1}{2}\left|\left\|\rho_{1,\beta} - \rho_{2,\beta} - (\rho_{1,\beta} - \tilde{\rho}_{1,\beta})\right\|_{\mathrm{tr}} - \left\|\tilde{\rho}_{2,\beta} - \rho_{2,\beta}\right\|_{\mathrm{tr}}\right| \\
&\geq \frac{1}{2}\left|\left|\left\|\rho_{1,\beta} - \rho_{2,\beta}\right\|_{\mathrm{tr}} - \left\|\rho_{1,\beta} - \tilde{\rho}_{1,\beta}\right\|_{\mathrm{tr}}\right| - \left\|\tilde{\rho}_{2,\beta} - \rho_{2,\beta}\right\|_{\mathrm{tr}}\right| \\
&\geq \frac{3}{4} - 2\epsilon \geq \frac{2}{3}
\end{aligned}$$

when $\epsilon \leq \frac{1}{24}$, which means that $\tilde{\rho}_{1,\beta}$ and $\tilde{\rho}_{2,\beta}$ can be distinguished with success probability $\geq 2/3$. Hence, if $\tilde{\rho}_{i,\beta}$ can be constructed using the block-encoding U_i of H_i, we have a distinguisher for unitary channels associated with U_i for $i \in \{1,2\}$.

The SVDs of H_1 and H_2 are $\mathbb{I}H_1\mathbb{I}$ and $\mathbb{I}H_2\mathbb{I}$, since both are diagonal and PSD. Using Eq. (20) we can construct the following two block-encodings of H_1 and H_2:

$$U_1 = \begin{bmatrix}
\frac{1}{2}+\frac{1}{\beta} & 0 & \sqrt{1-\left(\frac{1}{2}+\frac{1}{\beta}\right)^2} & 0 \\
0 & \frac{1}{2}-\frac{1}{\beta} & 0 & \sqrt{1-\left(\frac{1}{2}-\frac{1}{\beta}\right)^2} \\
\sqrt{1-\left(\frac{1}{2}+\frac{1}{\beta}\right)^2} & 0 & -\frac{1}{\beta}-\frac{1}{2} & 0 \\
0 & \sqrt{1-\left(\frac{1}{2}-\frac{1}{\beta}\right)^2} & 0 & \frac{1}{\beta}-\frac{1}{2}
\end{bmatrix},$$

$$U_2 = \begin{bmatrix}
\frac{1}{2}-\frac{1}{\beta} & 0 & \sqrt{1-\left(\frac{1}{2}-\frac{1}{\beta}\right)^2} & 0 \\
0 & \frac{1}{2}+\frac{1}{\beta} & 0 & \sqrt{1-\left(\frac{1}{2}+\frac{1}{\beta}\right)^2} \\
\sqrt{1-\left(\frac{1}{2}-\frac{1}{\beta}\right)^2} & 0 & -\frac{1}{\beta}+\frac{1}{2} & 0 \\
0 & \sqrt{1-\left(\frac{1}{2}+\frac{1}{\beta}\right)^2} & 0 & -\frac{1}{\beta}-\frac{1}{2}
\end{bmatrix}.$$

Evaluating the operator norm distance of U_1 and U_2 gives us

$$\left\|U_1 - U_2\right\|_{\mathrm{op}} = \frac{\sqrt{3\beta^2 - \sqrt{9\beta^4 - 40\beta^2 + 16} + 4}}{\sqrt{2}\beta} \leq \frac{3}{\beta}$$

for $\beta \geq \sqrt{\frac{14}{3}}$. Moreover, for these values of β we have $\left\|U_1 - U_2\right\|_{\mathrm{op}} \leq \frac{3}{\sqrt{14/3}} \leq 1.4$, which means that $0 \notin \mathrm{conv}(\mathrm{eig}(U_1^\dagger U^2)$ by Lemma 4. Therefore, by Lemma 3 we then have $T \geq \Omega(\beta)$. □

This matches the upper bound of the known quantum Gibbs samplers, see for example Ref. [53].

4.2.2 No fast-forwarding for Hamiltonian simulation

In Hamiltonian simulation one has access to some Hamiltonian H and is given a time $t \in \mathbb{R}$, with the goal of implementing the unitary $\tilde{U}$ which approximates $U = e^{-itH}$ up to diamond distance ϵ. It is well-known that it is generally not possible to do so-called Hamiltonian *fast-forwarding*, which refers to a Hamiltonian simulation algorithm which implements the $\tilde{U}$ in time sub-linear in t [17].

Claim 5 (No fast-forwarding for Hamiltonian simulation)**.** *Let H with $\|H\|_{\text{op}} \leq 1$ be some Hamiltonian to which we have access through a block-encoding U_H. Suppose $t \geq 1/2\pi$. Then it takes at least*

$$T \geq \Omega(t)$$

queries to U_H to implement e^{-iHt} up to diamond distance $\leq 1/3$.

Proof. Let $H_1 = \frac{I_2}{2}$, and $H_2 = H_1 + \frac{1}{2t} |1\rangle\langle 1|$, such that $\|H_1\|_{\text{op}} \leq 1$ and $\|H_2\|_{\text{op}} \leq 1$. Define $t = 2\pi t'$ with $t' \geq 0$. Suppose we could implement $U_i = e^{-iH_i t}$ perfectly for $i \in \{1, 2\}$. We then have that

$$e^{-2\pi i H_1 t'} |+\rangle = e^{-i\pi t'} |+\rangle$$

and

$$e^{-2\pi i H_2 t'} |+\rangle = e^{-i\pi t'} |-\rangle ,$$

which are perfectly distinguishable by a measurement in the Hadamard basis. If instead we can implement some $\tilde{U}_i$ such that $\frac{1}{2} \left\| \tilde{U}_i - U_i \right\|_\diamond \leq 1/3$ for $i \in \{1, 2\}$, our Hadamard basis measurement will be able to distinguish both cases with success probability $\geq 2/3$. Hence, we have that a Hamiltonian simulation algorithm that uses U_H as a subroutine can be used to distinguish U_{H_1} from U_{H_2}. For the block-encodings of H_1 and H_2 we have

$$U_1 = \begin{bmatrix} \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & 0 & -\frac{1}{2} \end{bmatrix}, \quad U_2 = \begin{bmatrix} \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & 0 \\ 0 & \frac{1+1/t'}{2} & 0 & \sqrt{1 + \left(\frac{1}{2} + \frac{1}{2t'^2}\right)^2} \\ \frac{\sqrt{3}}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & \sqrt{1 + \left(\frac{1}{2} + \frac{1}{2t'^2}\right)^2} & 0 & -\frac{1+1/t'}{2} \end{bmatrix},$$

respectively. Again by Lemma 3, evaluating the operator distance we find

$$\|U_1 - U_2\|_{\text{op}} = \frac{\sqrt{3 - \sqrt{-\frac{3}{t'^2} - \frac{6}{t'} + 9} - \frac{1}{t'}}}{\sqrt{2}} \leq \frac{1}{t'},$$

for which the inequality can be shown to hold after some straightforward algebraic manipulation, assuming that $t' \geq 1$. Again, for $t' \geq 1$ (and thus $t \geq 1/2\pi$) we have $\|U_1 - U_2\|_{\text{op}} \leq 1 \leq 1.4$, so $0 \notin \text{conv}(\text{eig}(U_1^\dagger U^2)$ by Lemma 4. Hence, by Theorem 1, $T = \Omega(t)$. □

See Ref. [41] for a matching upper bound in the simulation time t.

4.2.3 Hamiltonian learning in the Heisenberg limit

In Hamiltonian learning, the problem is to output a classical description of a Hamiltonian H' that is ϵ-close to H with respect to some distance measure d in the space of Hamiltonians, with probability $\geq$ by making queries to its time evolution operator $U(t) = e^{-itH}$, where $t \geq 0$ is tunable. The total evolution time is then defined as the sum of all different evaluation times used in the different queries. As a distance measure, we will take the operator norm distance $\left\|\tilde{H} - H\right\|_{\text{op}}$.

Claim 6. *Given access to an unknown Hamiltonian H with $\|H\|_{\text{op}} \leq 1$ through its time evolution operator $U(t) = e^{-itH}$, with $t \geq 0$ a tunable parameter, outputting the matrix description of a $\tilde{H}$ such that $\left\|\tilde{H} - H\right\|_{\text{op}} \leq \epsilon$, where $0 < \epsilon \leq \frac{1}{2}$, requires a total evolution time of at least $\Omega(1/\epsilon)$.*

Proof. Let $H_1 = \mathbb{I}$ and $H_2 = \mathbb{I} - 2\epsilon\,|0\rangle\langle 0|$. Since $0 < \epsilon \leq \frac{1}{2}$, we have $\|H_1\|_{\text{op}} \leq 1$ and $\|H_2\|_{\text{op}} \leq 1$ holds. Learning an unknown U up to ϵ in operator distance allows one to distinguish H_1 from H_2. Suppose that we make m queries to the time evolution operator, each with some evolution time t_j with $j \in [m]$. We have that $U_1(t) = e^{-it_j}\mathbb{I}$ and

$$U_2(t_j) = \begin{bmatrix} e^{-it_j(1-2\epsilon)} & 0 \\ 0 & e^{-it_j} \end{bmatrix}.$$

We have that

$$U_1(t_j)^\dagger U_2(t_j) = \begin{bmatrix} e^{2it_j\epsilon} & 0 \\ 0 & 1 \end{bmatrix}.$$

which means that $D = \frac{1}{2}|1 + e^{2it_j\epsilon}|$. Now suppose that $t_j \geq \frac{\pi}{2\epsilon}$. Then this would match our desired lower bound. However, if $t_j\epsilon < \frac{\pi}{2\epsilon}$, the condition $0 \notin \text{conv}(\text{eig}(U_1^\dagger U_2))$ is satisfied. Therefore, by Lemma 2 we have

$$\frac{1}{2}\left\|\mathcal{U}(U_1(t_j)) - \mathcal{U}(U_2(t_j))\right\|_\diamond = \sqrt{1 - D^2} = |\sin(t_j\epsilon)| \leq t_j\epsilon.$$

The proof of Theorem 1 then directly implies that $T = \sum_{j\in[m]} t_j = \Omega(1/\epsilon)$. □

See Ref. [20] for a (local) Hamiltonian learning algorithm which achieves the Heisenberg scaling for its total evolution time.

4.2.4 Ground state preparation of spectrally-gapped Hamiltonians

In approximate ground state preparation problems one is given a Hamiltonian H with some unknown ground state $|\psi\rangle$, for which one has to prepare a state $|\psi\rangle$ such that $|\langle\psi_0|\psi\rangle|^2 \geq 1 - \epsilon$. It is well known that the *spectral gap* $\gamma(H)$, that is the difference between the energies of the ground state and the first excited state of H, plays an important role in how difficult this problem is [21, 54, 55].

Claim 7 (Spectrally gapped ground state preparation)**.** *Let H with $\|H\|_{\text{op}} \leq 1$ be some Hamiltonian to which we have access through a block-encoding U_H. Suppose $\gamma(H) \geq \Delta$ for some $0 < \Delta \leq 1$. Then it takes at least*

$$T \geq \Omega(1/\Delta)$$

queries to U_H to implement a state $|\phi\rangle$ which approximates the ground state $|\psi\rangle$ up to fidelity $\geq 2/3$.

Proof. For a Hilbert space $\mathcal{H} := \mathbb{C}^3$, let $H_1 = \Delta\,|1\rangle\langle 1| + |2\rangle\langle 2|$ and $H_2 = \Delta\,|0\rangle\langle 0| + |2\rangle\langle 2|$. Since $0 < \Delta \leq 1$, we have that $\|H_1\|_{\text{op}} \leq 1$ and $\|H_2\|_{\text{op}} \leq 1$ holds. The ground states of H_1 and H_2 are given by $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = |1\rangle$, respectively. Note that indeed $\gamma(H_1) = \gamma(H_2)) = \Delta$. Suppose that we have an algorithm could prepare the ground state of an unknown H up to fidelity $\geq 2/3$ by making queries to the block-encoding of H, then we could distinguish H_1 from H_2 by preparing the ground state and performing a measurement $\{|0\rangle\langle 0|\,, \mathbb{I} - |0\rangle\langle 0|\}$. For some real number $c = |\langle\phi|\psi\rangle|$ with $|c|^2 \geq 2/3$, and $\theta \in [0, 1]$, we can write the prepared state as $|\phi\rangle = ce^{i\theta}\,|\psi\rangle + (1-c)|\psi^{\perp}\rangle$, where $|\psi^{\perp}\rangle$ lives in the space orthogonal to $|\psi\rangle$. Clearly, if $|\psi\rangle = |0\rangle$ then we have that $|\,\langle\phi|0\rangle\,| = |c|^2 \geq 2/3$ and when $|\psi\rangle = |1\rangle$ then $|\,\langle\phi|0\rangle\,|^2 \leq 1 - |c|^2 \leq 1/3$. Therefore, we have that the probability of measuring $|0\rangle$ when $H = H_1$ is $\geq 2/3$ and when $H = H_2$ it is $\leq 1/3$, which means that we can distinguish between both cases with an overall success probability $\geq 2/3$. For the block-encodings of H_1 and H_2 we have

$$U_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & \Delta & 0 & 0 & \sqrt{1-\Delta^2} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{1-\Delta^2} & 0 & 0 & -\Delta & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad U_2 = \begin{bmatrix} 0 & 0 & 0 & \sqrt{1-\Delta^2} & 0 & 0 \\ 0 & \Delta & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \sqrt{1-\Delta^2} & 0 & 0 & -\Delta & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

A direct computation shows that

$$\|U_1 - U_2\|_{\text{op}} = \frac{1}{2}\left(\Delta + \sqrt{8 - 3\Delta^2 - 8\sqrt{1-\Delta^2}}\right) \leq 2\Delta.$$

For $\Delta \leq 0.7$ we therefore have that $\|U_1 - U_2\|_{\text{op}} \leq 1/4$ and thus, by virtue of Lemma 4, $0 \notin \text{conv}(\text{eig}(U_1^{\dagger}U_2))$. By Theorem 1, $T \geq \Omega(1/\Delta)$. □

For an algorithm that uses H in its block-encoding and achieves $\tilde{\mathcal{O}}(1/\Delta)$ scaling, see Ref. [21].

5 Quantum oracle separations with SBQP

In this section we will give the proofs of Theorem 2 and Theorem 3. We will first argue that lower bounds on unitary property testing in general can be used to show quantum oracle separations using the following strategy: Take a language L which is not in C_1 nor in C_2 (if it already is in C_1, then it already implies a separation). Define a unitary property $\mathcal{P} = (U_{\text{yes}}, U_{\text{no}})$ in such a way that for a family of quantum oracles $\{U_x\}$, parametrised by the input x, the following two conditions hold:

1. If $x \in L$, then $U_x \in U_{\text{yes}}$ and if $x \notin L$, then $U_x \in U_{\text{no}}$.
2. To decide whether $U_x \in U_{\text{yes}}$ or $U_x \in U_{\text{no}}$ can be done in C_1 (i.e. it does not exceed the maximum allowed query complexity) but not in C_2 (it does exceed the maximum allowed query complexity for all $n \geq n_0$, for some $n_0 \in \mathbb{N}$).

One can then use the standard technique of diagonalization [56] to show a quantum oracle separation between C_1 and C_2. However, in our case, it turns out the separation can be shown in an even simpler way. Since we want oracle separations with SBQP, we can construct an oracle that is very close in diamond distance to the identity operator. For any class that makes only a polynomial number of queries and can only distinguish between

inverse polynomial output probabilities (and has error reduction), the unitary oracle will look just like the identity operator at large values of n. Hence, if a language L is not in C_2, it will also not be in C_2^U since this would imply that it would also be in $\mathsf{C}_2^{\mathbb{I}} = \mathsf{C}_2$. We will need the following lemma of one-bit quantum phase estimation to show containment in SBQP.

Lemma 7 (One-bit quantum phase estimation [27])**.** *Let $U \in \mathbb{U}(2^n)$ and $|\psi\rangle$ a n-dimensional quantum state (which can be prepared exactly in an efficient manner) such that $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$, for some $\theta \in [0,1)$. Then there exists a quantum algorithm that makes one controlled query to U and outputs 1 with probability $\sin^2(\pi\theta)$.*

Proof. The one-bit quantum phase estimation circuit for a n-qubit unitary starts with $n+1$ qubits initialised in $|0\rangle|\psi\rangle$, applies a Hadamard to the first qubit, followed by an application of U to the remaining n qubits controlled on the first qubit, and finishes by applying yet another Hadamard to first qubit followed by a measurement in the computational basis of this qubit. We have that the output state of the one-bit quantum phase estimation circuit is given by

$$\frac{1}{2}(|0\rangle + |1\rangle)|\psi\rangle + \frac{e^{2\pi i\theta}}{2}(|0\rangle - |1\rangle)|\psi\rangle,$$

which means that the probability of measuring '1' as a function of $\theta \in [0,1)$ can be expressed as

$$\Pr[\text{One-bit QPE outputs 1}] = \left|\frac{1 - e^{2i\pi\theta}}{2}\right|^2 = \sin^2(\pi\theta).$$

□

We are now ready to state the proof, which uses the above argument to turn the lower bound of Claim 1 into a quantum oracle separation.

Theorem 2. *There exists a quantum oracle U such that*

$$\mathsf{QMA}(2)^U \not\supset \mathsf{SBQP}^U.$$

Proof. Since $\mathsf{QMA}(2) \subseteq \mathsf{NEXP}$, we have that there must exist a unary language L for which it holds that $L \notin \mathsf{QMA}(2)$. Pick any such L, let $p(n)$ be some polynomial and define the quantum oracle $U = \{U_n\}_{n\geq 1}$ with $U_n = e^{2\pi i\theta_n}|0\rangle\langle 0| + |1\rangle\langle 1|$ for some $\theta_n \in [0,1)$ as follows:

- if $0^n \in L$, then $\theta_n = 2^{-p(n)}$.
- if $0^n \notin L$, then $\theta_n = 0$.

Clearly, we have that $L \in \mathsf{SBQP}^U$ since we have that running the one-bit quantum phase estimation protocol from Lemma 7 with U and $|\psi\rangle = |0\rangle$, saying that it accepts when it outputs '1', satisfies

- if $0^n \in L$, then $\Pr[\text{One-bit QPE accepts}] = \sin^2(\pi 2^{-p(n)}) \geq 2^{-2p(n)} \geq 2^{-p'(n)}$,
- if $0^n \notin L$, then $\Pr[\text{One-bit QPE accepts}] = 0 \leq 2^{-p'(n)-1}$,

for some polynomial $p'(n)$. We will now show that $L \notin \mathsf{QMA}(2)^U$. Let $q(n)$ be a polynomial which is an upper bound on the runtime of the $\mathsf{QMA}(2)^U$ verifier. Now observe that the identity operator has diamond distance $\leq \pi 2^{-p'(n)}$ from the oracle U_n. Hence, if we replace the oracle U with the identity operator $\mathbb{I}$ in all the $\mathsf{QMA}(2)^U$ verifiers V^U, we have that by Theorem 1 that

$$\left|\Pr\left[V^{U_n} \text{ accepts } (x, |\psi_1\rangle \otimes |\psi_2\rangle)\right] - \Pr\left[V^{\mathbb{I}} \text{ accepts } (x, |\psi_1\rangle \otimes |\psi_2\rangle)\right]\right| \leq \frac{\pi q(n)}{2^{p'(n)}} \leq 0.01,$$

for all $n \geq n_0$, with n_0 some constant that only depends on the choices of the polynomials $p(n), q(n)$. Hence, this implies that if $L \in \mathsf{QMA}(2)^U$, then it must also be that $L \in \mathsf{QMA}(2)$, since one can use the oracle for all $n < n_0$ making at most $2^{p'(n_0)}$ queries (which is constant for a constant n_0) and simply replace the oracle with the identity operator for all $n \geq n_0$, whilst still having a bounded probability of error (and apply error reduction as in Ref. [22] to boost it back to $\geq 2/3$). But this contradicts the fact that we have picked L such that it was not in $\mathsf{QMA}(2)$. □

Theorem 3. *There exists a quantum oracle U such that*

$$\mathsf{QMA/qpoly}^U \not\supset \mathsf{SBQP}^U.$$

Proof. This follows from a similar proof as Theorem 2, but now we choose a binary language L (to be specified later). Let the quantum oracle $U = \{U_x\}_{x\in\{0,1\}^n, n\geq 1}$ with $U_x = e^{2\pi i\theta_x} |0^n\rangle \langle 0^n| + (\mathbb{I} - |0^n\rangle \langle 0^n|)$ be a family of $n(= |x|)$-qubit unitaries parametrized by some $\theta_x \in [0, 1)$, which is given as follows:

$$\theta_x = \left(1 + (-1)^{L(x)}\right) 2^{-p(|x|)-1},$$

where $L(x) = 1$ if $x \in L$ and $L(x) = 0$ otherwise. Hence, we have that

- If $x \in L$, then $\theta_x = 0$;
- If $x \notin L$, then $\theta_x = 2^{-p(|x|)}$.

Clearly, $L \in \mathsf{SBQP}^U$ for any choice of language L by the same argument as in Theorem 2. Observe that the lower bound of Claim 1 also hold for these specific instances of U where the number of qubits it acts on varies, as the diamond distance only changes with different n because the eigenphases change with different values of n (if $\theta = \epsilon$ for some fixed $\epsilon > 0$, then the diamond distance would be fixed for all n). Since $\mathsf{QMA/qpoly} \subseteq \mathsf{PSPACE/poly} \neq \mathsf{ALL}$ [29], we can use the same argument as in Theorem 2 to show that there must exist a $L \notin \mathsf{QMA/qpoly}^U$. □

Note that it is not clear if we can combine both unentangled quantum proofs as advice and arrive at a similar oracle separation, as we do not know whether $\mathsf{QMA}(2)/\mathsf{qpoly} = \mathsf{ALL}$ or not [29], so it might be that no language L exists such that $L \notin \mathsf{QMA}(2)/\mathsf{qpoly}$.

References

[1] Guoming Wang. Property testing of unitary operators. *Phys. Rev. A*, 84:052328, Nov 2011. arXiv: 1110.1133. 1, 6

[2] Adrian She and Henry Yuen. Unitary Property Testing Lower Bounds by Polynomials. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251, pages 96:1–96:17, 2023. arXiv: 2210.05885. 1, 2, 7, 8, 9

[3] Thomas Chen, Shivam Nadimpalli, and Henry Yuen. Testing and Learning Quantum Juntas Nearly Optimally. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1163–1185, 2003. arXiv: 2207.05898. 1, 7

[4] Qisheng Wang and Zhicheng Zhang. Quantum lower bounds by sample-to-query lifting, August 2023. arXiv: 2308.01794. 1, 4, 7, 18, 19

[5] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. ISBN 0897917855. arXiv: quant-ph/9605043. 1

[6] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and Weaknesses of Quantum Computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. arXiv: quant-ph/9701001. 1

[7] Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 115–128, 2007. arXiv: quant-ph/0604056. 1, 7

[8] A. Acín. Statistical Distinguishability between Unitary Operations. *Phys. Rev. Lett.*, 87:177901, Oct 2001. arXiv: quant-ph/0102064. 2, 3

[9] G. Mauro D'Ariano, Paoloplacido Lo Presti, and Matteo G. A. Paris. Using Entanglement Improves the Precision of Quantum Measurements. *Phys. Rev. Lett.*, 87:270404, Dec 2001. arXiv: quant-ph/0109040. 2

[10] Runyao Duan, Yuan Feng, and Mingsheng Ying. Entanglement is Not Necessary for Perfect Discrimination between Unitary Operations. *Phys. Rev. Lett.*, 98:100503, Mar 2007. arXiv: quant-ph/0601150. 2, 3

[11] Mário Ziman and Michal Sedlák. Single-shot discrimination of quantum unitary processes. *Journal of Modern Optics*, 57(3):253–259, 2010. arXiv: 1003.1488. 2, 11

[12] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. 2, 11

[13] Murray J Holland and Keith Burnett. Interferometric detection of optical phase shifts at the Heisenberg limit. *Physical review letters*, 71(9):1355, 1993. 3

[14] ZY Ou. Complementarity and fundamental limit in precision phase measurement. *Physical review letters*, 77(12):2352, 1996. 3

[15] Arvid J. Bessen. Lower bound for quantum phase estimation. *Phys. Rev. A*, 71: 042313, Apr 2005. arXiv: quant-ph/0412008. 3, 5

[16] Ashwin Nayak and Felix Wu. The quantum query complexity of approximating the median and related statistics. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, STOC '99, page 384–393, 1999. ISBN 1581130678. arXiv: quant-ph/9804066. 5, 16

[17] Dominic W Berry, Graeme Ahokas, Richard Cleve, and Barry C Sanders. Efficient quantum algorithms for simulating sparse Hamiltonians. *Communications in Mathematical Physics*, 270:359–371, 2007. arXiv: quant-ph/0508139. 5, 24

[18] Chi-Fang Chen, Michael J Kastoryano, Fernando GSL Brandão, and András Gilyén. Quantum Thermal State Preparation, March 2023. arXiv: 2303.18224. 5, 22

[19] Nikhil S. Mande and Ronald de Wolf. Tight Bounds for Quantum Phase Estimation and Related Problems. In *31st Annual European Symposium on Algorithms (ESA 2023)*, volume 274, pages 81:1–81:16, 2023. ISBN 978-3-95977-295-2. arXiv: 2305.04908. 5, 7

[20] Hsin-Yuan Huang, Yu Tong, Di Fang, and Yuan Su. Learning many-body Hamiltonians with Heisenberg-limited scaling. *Physical Review Letters*, 130(20):200403, 2023. 5, 25

[21] Lin Lin and Yu Tong. Near-optimal ground state preparation. *Quantum*, 4:372, December 2020. ISSN 2521-327X. arXiv:2002.12508. 5, 25, 26

[22] Aram W. Harrow and Ashley Montanaro. Testing Product States, Quantum Merlin-Arthur Games and Tensor Optimization. *J. ACM*, 60(1), February 2013. ISSN 0004-5411. arXiv: 1001.0017. 5, 9, 10, 28

[23] Yi-Kai Liu, Matthias Christandl, and Frank Verstraete. Quantum Computational Complexity of the N-Representability Problem: QMA Complete. *Phys. Rev. Lett.*, 98:110503, Mar 2007. arXiv: quant-ph/0609125. 5

[24] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 223–236, 2008. arXiv: 0804.0802. 5

[25] Salman Beigi. NP vs $\mathrm{QMA}_{\log}(2)$. *Quantum Information & Computation*, 10(1):141–151, 2010. arXiv: 0810.5109. 5

[26] Hugue Blier and Alain Tapp. All Languages in NP Have Very Short Quantum Proofs. In *2009 Third International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, 2009. arXiv: 0709.0738. 5

[27] Alexei Y. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. *Electron. Colloquium Comput. Complex.*, TR96, 1995. arXiv: quant-ph/9511026. 6, 17, 27

[28] Bill Fefferman and Cedric Lin. Quantum Merlin Arthur with exponentially small gap, 2016. arXiv: 1601.01975. 6

[29] Scott Aaronson. QMA/qpoly $\subseteq$ PSPACE/poly: de-Merlinizing quantum protocols. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 13 pp.–273, July 2006. DOI: 10.1109/CCC.2006.36. arXiv: quant-ph/0510230. 6, 28

[30] Harry Buhrman, Lance Fortnow, Ilan Newman, and Hein Röhrig. Quantum property testing. *SIAM Journal on Computing*, 37(5):1387–1400, 2008. arXiv: quant-ph/0201117. 6

[31] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, July 2001. ISSN 0004-5411. arXiv: quant-ph/9802049. 6

[32] Andris Ambainis. Quantum Lower Bounds by Quantum Arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002. ISSN 0022-0000. arXiv: quant-ph/0002066, Earlier version in STOC'00. 6

[33] Samuel Kutin. Quantum Lower Bound for the Collision Problem with Small Range. *Theory of Computing*, 1(2):29–36, 2005. arXiv: quant-ph/0304162. 6

[34] A. Ambainis. Polynomial degree vs. quantum query complexity. In *44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings.*, pages 230–239, 2003. arXiv: quant-ph/0305028. 6

[35] Peter Hoyer, Troy Lee, and Robert Spalek. Negative weights make adversaries stronger. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, page 526–535, 2007. ISBN 9781595936318. arXiv: quant-ph/0611054. 6

[36] Ben W. Reichardt. Span Programs and Quantum Query Complexity: The General Adversary Bound Is Nearly Tight for Every Boolean Function. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 544–551, 2009. arXiv: 0904.2759. 6

[37] Aleksandrs Belovs. Variations on quantum adversary, April 2015. arXiv: 1504.06943. 7

[38] Ashley Montanaro and Ronald de Wolf. A Survey of Quantum Property Testing. *Theory of Computing*, 2016, 10 2013. arXiv: 1310.2035. 7, 8

[39] Dorit Aharonov, Jordan Cotler, and Xiao-Liang Qi. Quantum algorithmic measurement. *Nature communications*, 13(1):887, 2022. arXiv: 2101.04634. 7

[40] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature physics*, 10(9):631–633, 2014. 7

[41] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC '19, page 193–204, 2019. ISBN 9781450367059. arXiv: 1806.01838. 7, 24

[42] Kean Chen, Qisheng Wang, and Zhicheng Zhang. Local test for unitarily invariant properties of bipartite quantum states, 2024. arXiv: 2404.04599. 7

[43] Michael M Wolf. Mathematical Introduction to Quantum Information Processing, March 2023. 12

[44] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. Query-optimal estimation of unitary channels in diamond distance. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 363–390, Los Alamitos, CA, USA, nov 2023. arXiv: 2302.14066. 12

[45] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge University Press, 2012. 14

[46] Steph Foulds, Viv Kendon, and Tim Spiller. The controlled SWAP test for determining quantum entanglement. *Quantum Science and Technology*, 6(3):035002, 2021. 18

[47] Peter Høyer. Arbitrary phases in quantum amplitude amplification. *Phys. Rev. A*, 62:052304, Oct 2000. arXiv: quant-ph/0006031. 19

[48] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum Fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001. arXiv: quant-ph/0102001. 19

[49] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Algorithms and Computation: 14th International Symposium, ISAAC 2003, Kyoto, Japan, December 15-17, 2003. Proceedings 14*, pages 189–198, 2003. 19

[50] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002. arXiv: quant-ph/0005055. 19, 21

[51] Guang Hao Low and Isaac L Chuang. Optimal Hamiltonian simulation by quantum signal processing. *Physical review letters*, 118(1):010501, 2017. 22

[52] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019. 22

[53] Chi-Fang Chen, Michael J Kastoryano, and András Gilyén. An efficient and exact noncommutative quantum Gibbs sampler, November 2023. arXiv: 2311.09207. 23

[54] Itai Arad, Zeph Landau, Umesh Vazirani, and Thomas Vidick. Rigorous RG algorithms and area laws for low energy eigenstates in 1D. *Communications in Mathematical Physics*, 356:65–105, 2017. 25

[55] Abhinav Deshpande, Alexey V. Gorshkov, and Bill Fefferman. The importance of the spectral gap in estimating ground-state energies. *PRX Quantum*, 3(4):040327, December 2022. arXiv:2207.10250. 25

[56] Theodore Baker, John Gill, and Robert Solovay. Relativizations of the P=?NP question. *SIAM Journal on computing*, 4(4):431–442, 1975. 26